LAUREA AMMATTIKORKEAKOULU Uuden edellä

Yleisen tietoturvallisuusohjeen kehittäminen poliisin henkilöstölle

Tirronen, Kari

2013 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Yleisen tietoturvallisuusohjeen kehittäminen poliisin henkilöstölle

Kari Tirronen
Turvallisuusosaamisen koulutus-ohjelma
Opinnäytetyö
Tammikuu, 2013

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Turvallisuusosaamisen koulutusohjelma
Ylempi ammattikorkeakoulututkinto

Kari Tirronen

Yleisen tietoturvallisuusohjeen kehittäminen poliisin henkilöstölle

Vuosi 2013 Sivumäärä 83

Poliisin tietoturvallisuus perustuu viranomaisen toiminnan julkisuudesta annetun lain ja asetuksen lisäksi useisiin muihin lakeihin. Poliisihallinnossa käsitellään runsaasti sekä julkista että salassa pidettävää tietoa, joten tietoturvallisuus on hoidettava asianmukaisesti. Tietoturvallisuus on jokaisen organisaatiossa työskentelevän velvollisuus ja se on juuri niin hyvä kuin on sen heikoin lenkki.

Poliisihallinnossa on lukuisia erilaisia ohjeita ja määräyksiä, joilla ohjataan tietoturvallisuutta. Ongelmana on se, että nämä ohjeet ja määräykset sijaitsevat hajallaan eri paikoissa ja niitä on joskus hyvin hankalaa ellei jopa mahdotonta löytää silloin kun niitä tarvittaisiin.

Tämän kehittämistyön tavoitteena on tuottaa poliisihallintoon yleinen tietoturvallisuusohje henkilöstön käyttöön. Tietoturvallisuusohjeeseen kootaan yhteen henkilöstön kannalta keskeisimmät tietoturvallisuusmääräykset ja –ohjeet. Ohje laaditaan sellaiseen muotoon, että sitä voidaan käyttää valtakunnallisesti, riippumatta poliisilaitoksesta tai poliisin yksiköstä. Tietoturvallisuusohjeen toteutuksessa pyritään ohjeiden käytännönläheisyyteen ja selkeyteen, sekä siihen, että ohjeet eivät ole ristiriidassa olemassa olevien ohjeiden ja määräysten kanssa.

Tietoturvallisuusohjeen kehittäminen on toteutettu tutkimuksellisena kehittämistyönä, joka lähtee organisaation kehittämistarpeesta. Kehittämistyötä varten käytiin läpi aiheeseen liittyvä materiaali ja määriteltiin poliisin henkilöstön kannalta keskeiset viitekehykset, käsitteet ja määritelmät, joiden pohjalta laadittiin yleinen tietoturvallisuusohje poliisin henkilöstölle.

Tietoturvallisuusohje sisältää tavanomaiset, jokapäiväiseen työhön liittyvät ohjeet ja määräykset, jotka ovat valtakunnallisesti käytettävissä, riippumatta poliisilaitoksesta tai yksiköstä. Ohjeen avulla on mahdollista kehittää ja yhdenmukaistaa poliisin tietoturvakäytäntöjä. Ohje auttaa lisäämään henkilöstön tietoturvatietoutta ja sitä voidaan myös käyttää apuna henkilöstölle suunnatun tietoturvakoulutuksen suunnittelussa.

Aikataulusyistä tietoturvallisuusohjeen käyttöönotto on kesken, eikä kehittämistyön toimivuutta ole mahdollista vielä arvioida.

Asiasanat: tietoturvallisuus, tietoturvallisuusohje, salassa pidettävä, suojaustaso, henkilötieto, tietoaineisto

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Master's Degree Programme in Security Management

Kari Tirronen

The development of a general data security manual for the national police force of Finland

Year 2013 Pages 83

The data security of the police force is not only based upon the law that governs openness of police activity, but also upon other legislation. The police administration is required to process a great deal of both public and secure information therefore data protection needs to be fit for purpose. Data security is the responsibility of each and every individual that works in the organization, and is only as strong as its weakest link.

The police administration has various existing rules to regulate the protection of data. The problem is that the material that contains these rules is scattered in many locations and is sometimes difficult, if not impossible, to find when the need arises.

The purpose of this project is to create a general data security manual for the administration. It will consist of the most relevant instructions for data security in a form that is universal, and is applicable regardless of the unit or its geographical location. The guidelines used in constructing the manual are practicality and clarity, and the need to avoid conflict with the current instructions.

This project has been carried out as research and development that is based upon the organization's need to evolve. The essential concepts, with key attributes and frameworks, were determined and the general data security manual was designed around them.

The data security manual consists of rules and regulations for everyday work, and is applicable nationwide. With this manual it is possible to develop and standardise the various data security procedures of the police force. It also increases the general awareness and knowledge of the subject and will be a useful tool in structuring data security training.

For timetable reasons the data security manual is in the process of being introduced; therefore the performance cannot be evaluated as yet.

Key words: data protection, information assurance, data protection instructions, confidential, security level, personal data, data

Sisällys

1 Johdanto

Poliisin tietoturvapolitiikan (2010) mukaan poliisi on yksi yhteiskunnan turvallisuusstrategian kriittisiä toimijoita, jonka on pystyttävä säilyttämään toimintakykynsä kaikissa turvallisuustilanteissa. Ydinprosessien toimivuuden sekä toimintakyvyn säilyttämisen kannalta on tietoturvallisuuden ja tietotekniikan kriittisyys tunnistettu poliisihallinnossa ja sen vuoksi tietoturvallisuus toimii kiinteässä yhteistyössä poliisin valmiustoiminnan kanssa. (Poliisin tietoturvapolitiikka määräys 2010.)

Valtionhallinnon tietoturvallisuuden yhteisiä lähtökohtia ovat säädöksissä määritellyt tietoturvavelvoitteet, valtioneuvoston periaatepäätös valtion tietoturvallisuuden kehittämisestä, valtiovarainministeriön antamat linjaukset sekä muut linjaukset. Jokaisella organisaatiolla on vastuu oman toimintansa tietoturvallisuudesta. (Tietoturvallisuus 2012.) Poliisin tietoturvaperiaatteet noudattavat sisäasiainministeriön asettamia tietoturvallisuuden ja poliisin hallinnonalan tietoturvapolitiikan linjauksia.

Tietoturvallisuus perustuu viranomaisen toiminnan julkisuudesta annetun lain ja asetuksen lisäksi useisiin muihin lakeihin. Poliisihallinnossa käsitellään runsaasti sekä julkista että salassa pidettävää tietoa, joten tietoturvallisuus on hoidettava asianmukaisesti. Tietoturvallisuus on jokaisen organisaatiossa työskentelevän velvollisuus ja se on juuri niin hyvä kuin sen heikoin lenkki.

1.1 Tutkimusongelman määrittely

Poliisihallinnossa on paljon erilaisia tietoturvallisuuteen liittyviä määräyksiä ja ohjeita, joita löytyy mm. poliisin Intranetin sivustoilta, HALTIK:in internet -sivuilta sekä eri yksiköiden omilta verkkolevyasemilta jne. Tietoturvamääräyksiä ja ohjeita on usein hyvin hankala, ellei jopa mahdoton löytää, jos ei tiedä missä ne sijaitsevat. Lisäksi määräyksissä ja ohjeissa viitataan usein johonkin lakiin, asetukseen tai VAHTI -ohjeisiin, jotka taas löytyvät muualta kuin tietoturvaohjeet. Tietoturvaohjeissa ei usein myöskään kerrota, miten jokin tietoturvallisuuteen liittyvä asia olisi tehtävä. Usein ohjeissa mainitaan vain esimerkiksi: ”pidettävä huoli” tai tehtävä näin tai noin jne. eli ei kerrota miten asiat tulisi toteuttaa konkreettisesti.

Tämä kaikki on johtanut siihen, että poliisin henkilöstön on hyvin vaikea hahmottaa tietoturvallisuuden laajaa kokonaisuutta eikä heillä näin ollen ole mahdollisuutta toteuttaa tietoturvallisuuteen liittyviä asioita niin kuin ne on tarkoitus toteuttaa poliisissa. Puhakaisen (2006) mukaan organisaatioissa keskitytään liikaa tietoturvallisuuden teknisiin ja toiminnallisiin ratkaisuihin eikä tietoturvatietoisuutta edistetä järjestelmällisesti. Suuri osa hyvän tietoturvallisuuden toteuttamisesta on kuitenkin organisatorisia asioita, ohjeita ja toimintatapoja.

Ihmisten rooli on keskeinen ja vain osa tietoturvallisuudesta hoituu teknologian avulla. Kyrölä (2001, 28) toteaa, että tietoturvallisuusriskien hallinnasta vain 20 % taataan teknisin ratkaisuin ja 80% taataan työntekijöiden toiminnan ja esimiesten johtamisen tuloksena.

Poliisihallinnon tietoturvallisuuden toteutuksessa on keskitytty lähinnä teknisiin ratkaisuihin sekä niiden toteuttamiseen ja työntekijät eli ns. loppukäyttäjät sekä heidän tieto-taidon kehittäminen ja ylläpitäminen on jäänyt vähemmälle. Poliisihallinnolla ei ole tällä hetkellä käytössä yhtä yhteistä henkilöstölle tarkoitettua tietoturvallisuusohjetta, johon olisi koottu yhteen tärkeimmät henkilöstöä koskevat tietoturvallisuuteen liittyvät asiat. Poliisin eri yksiköt ovat toteuttaneet tietoturvallisuuden ohjeistuksen jokainen omalla tavallaan ja näin ei poliisissa ole yhdenmukaista käytäntöä tietoturvallisuuden ylläpitämiseksi ja parantamiseksi.

1.2 Kehittämistyön tavoitteet, hyödyt ja rajaus

Tämän kehittämistyön tavoitteena on tuottaa poliisihallintoon yleinen tietoturvaohje, joka on tarkoitettu henkilöstön eli ns. loppukäyttäjien perus tietoturvaohjeeksi. Tietoturvaohjeessa kuvataan perusvaatimukset sekä ohjataan tarvittaessa hakemaan lisätietoa muusta ohjeistuksesta. Ohje laaditaan sellaiseen muotoon, että se on käytettävissä valtakunnallisesti, riippumatta laitoksesta tai yksiköstä ja että se sopii niin kenttä- kuin toimistohenkilöstölle. Tietoturvaohjeen toteutuksessa pyritään ohjeiden käytännönläheisyyteen, selkeyteen ja yksinkertaisuuteen sekä siihen, että ohjeet eivät ole ristiriidassa olemassa olevien ohjeiden kanssa.

Yhteisen ohjeen avulla voidaan parantaa ja yhdenmukaistaa poliisihallinnon tietoturvakäytäntöjä. Sen avulla voidaan myös lisätä henkilöstön tietoturvatietoisuutta ja -taitoja sekä motivaatiota turvata tietoa. Tätä myötä henkilöstön toimintatavat voivat myös muuttua tietoturvallisempaan suuntaan. Lisäksi ohjetta voidaan käyttää myös apuna tietoturvakoulutuksen suunnittelussa.

Tietoturvaohjeen ensisijainen kohderyhmä on poliisin henkilöstö eli ns. loppukäyttäjät ja sen tavoitteena on olla apuna tietoturvallisuuteen liittyvissä asioissa heidän jokapäiväisessä työssään. Ohjetta voivat hyödyntää myös tietoturvallisuudesta vastaavat sekä kouluttajat soveltuvin osin. Ohjeessa ei paneuduta varsinaisiin tietoteknisiin ratkaisuihin eikä -asioihin, sillä niistä on olemassa omat ohjeensa ja oppaat niitä tarvitseville.

1.3 Kehittämisraportin rakenne

Luku 2 käsittää kehittämistyön teoreettisen taustan, joka pitää sisällään kehittämistyöhön liittyvät keskeiset käsitteet ja määritelmät sekä kehittämistyössä sovelletut keskeiset viitekehykset. Kolmannessa luvussa kuvataan kehittämistyön tutkimus- ja kehittämismenetelmät.

Kehittämistyön tuloksia tarkastellaan neljännessä luvussa ja 5 luku sisältää kehittämistyön arvioinnin ja luku 6 sisältää yhteenvedon kehittämistyöstä. Kehittämistyön lopputuloksena syntynyt Yleinen tietoturvaohje Poliisin henkilöstölle on raportissa erillisenä liitteenä.

2 Teoreettinen tausta

Tutkimusongelman ratkaisemisessa tutkimusmenetelmällä on merkittävä osuus. Tutkijan tehtävänä on valita vallitsevaan ongelmaan mielestään parhaiten soveltuva menetelmä. Menetelmän valintaan vaikuttaa myös tutkijan valitsema lähestymistapa. Yksi mahdollinen lähestymistapa on tehdä selvitys siitä, mitä kirjallista ja muuta aineistoa (esim. ohjeet, määräykset, lait jne.) aiheesta on olemassa ja selvittää millaisia käsitteitä aihe pitää sisällään. Tässä työssä käsitellään niitä keskeisiä tietoturvallisuuteen liittyviä käsitteitä ja viitekehyksiä, joita käytetään poliisihallinnossa tietoturvallisuudesta puhuttaessa.

Tämän kehittämistyön kohderyhmänä ovat organisaation eli poliisin työntekijät, jotka eivät ole tietoturvallisuuden ja siihen liittyvän terminologian ja käsitteiden asiantuntijoita. Käsitteitä ja termejä tarkastellaan siinä laajuudessa, kuin se on tarkoituksenmukaista henkilöstön tietoturvallisuustietouden lisäämisen kannalta.

2.1 Keskeiset käsitteet ja määritelmät

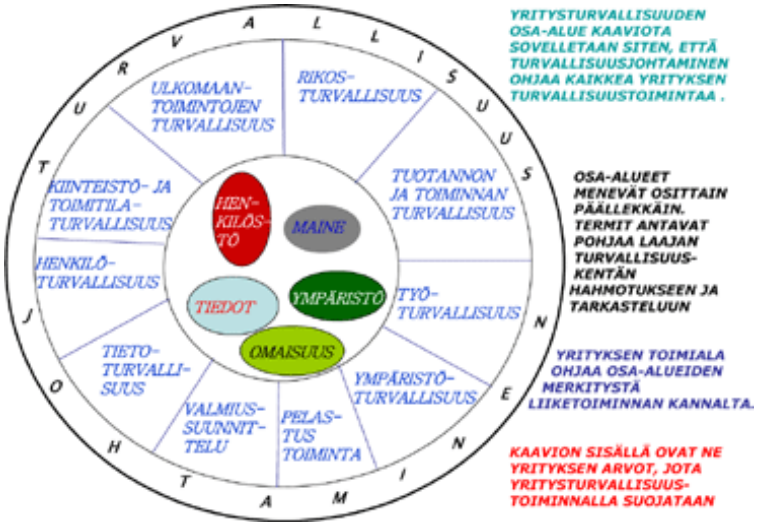
2.1.1 Yritys- ja organisaatioturvallisuus

Yritysturvallisuus tarkoittaa turvallisuuden eri osa-alueiden kokonaisvaltaista hallintaa. Se on kiinteä osa yrityksen toimintaa ja tukee omalta osaltaan yrityksen liiketoiminnan tulostavoitteita. (Miettinen 2002, 11.)

Yritysturvallisuus on yrityksen jokapäiväistä toimintaa ja siitä vastaa yrityksen johto. Sillä varmistetaan yrityksen toimintaedellytykset, toiminnan, tuotannon ja palveluiden häiriöttömyys, jatkuvuus sekä turvallinen toimintaympäristö. (Heljaste ym. 2008, 27.)

Organisaatioturvallisuus ei ole itsenäinen kokonaisuus, vaan se tarkoittaa niiden toimenpiteiden kokonaisuutta, joiden tavoitteena on häiriöttömän toiminnan varmistaminen – se on eräänlainen näkökulma ja työkalu, jonka avulla turvallisuutta ja riskejä voidaan hallita (Leppänen 2006, 59).

Yritysturvallisuus koostuu lukuisista eri turvallisuuden osa-alueista. Suomessa on yleisesti käytössä Yritysturvallisuuden neuvottelukunnan tekemä jaottelumalli organisaatioturvallisuuden määritelmistä (Kuvio: 1).



Kuvio 1: Yritysturvallisuuden osa-alueet (Yritysturvallisuuden neuvottelukunta 2009)

Riippumatta siitä minkälaisiin osa-alueisiin yritysturvallisuus jaetaan, huomataan että tietoturvallisuus on osa yritysturvallisuuden kokonaisuutta ja se sisältyy kaikkeen organisaatio- ja yritysturvallisuuteen. Jokaisella organisaatiolla organisaatio- / yritysturvallisuus käsittää hieman eri asioita riippuen toimialasta ja tehtävästä.

2.1.2 Turvallisuusjohtaminen ja tietoturvallisuuden johtaminen

Turvallisuusjohtaminen on kokonaisuus, jonka turvallisuusjohto muodostaa organisaation kaikista turvallisuuteen vaikuttavista osa-alueista. Turvallisuusjohtaminen sisältää kaikki ne toiminnot, joiden avulla varmistetaan organisaation tavoitteiden saavuttaminen ja suojattavien kohteiden vahingoittumattomuus. (Leppänen 2006, 57.)

Tietoturvallisuuden johtaminen on osa normaalia johtamista ja sillä on oltava selkeät yhtymäkohdat yrityksen muihin johtamistoimintoihin. Se ei siis saa olla erillinen osa yrityksen muuta johtamistoimintaa. (Miettinen 1999, 95.)

2.1.3 Tietoturvallisuus

Tietoturvallisuus on pieniä tekoja osana jokapäiväistä toimintaa ja se koskettaa organisaation jokaista työntekijää eikä vain esimiehiä tai tietotekniikasta vastuullista osastoa. Tietoturvallisuuden tulee olla osana organisaatiokulttuuria, jolloin kaikki ymmärtävät tietoturvallisuuden merkityksen ja työskentelevät sen saavuttamiseksi ja ylläpitämiseksi. (Laaksonen, Nevasalo, & Tomula 2006, 17–19.) Tietoturvallisuus koostuu tietoaineistoturvallisuudesta, hallinnollisesta ja fyysisestä tietoturvallisuudesta, tietoliikenne-, laitteisto-, ohjelmisto- ja käyttöturvallisuudesta. Ihmisillä ja heidän toiminnallaan on suuri merkitys, mutta teknistymisen myötä

myös tietoteknisillä ratkaisuilla on merkittävä rooli tietoturvallisuuden ylläpidossa.(Leppänen 2006, 260.)

Hakala, Vainio ja Vuorinen (2006, 4-6) määrittelevät tietoturvallisuuden kahdella eri tavalla, klassisen tiedon arvoon perustuvaan ja laajennettuun tietoturvallisuuden määritelmään.

Klassinen tiedon arvoon perustuva määritelmä	**Laajennettu tietoturvallisuuden määritelmä**
1. Luottamuksellisuus	1. Luottamuksellisuus
2. Käytettävyys	2. Käytettävyys
3. Eheys	3. Eheys
	4. Kiistämättömyys
	5. Pääsynvalvonta

Taulukko 1: Tietoturvallisuuden määritelmät (mukailtu Hakala & ym. 2006)

Luottamuksellisuudella tarkoitetaan, että tietojärjestelmän tiedot ovat vain niihin oikeutettujen henkilöiden käytettävissä. Käytettävyys merkitsee sitä, että tiedot ovat saatavissa tietojärjestelmästä oikeassa muodossa ja riittävän nopeasti. Eheys tarkoittaa sitä, että tietojärjestelmän tiedot pitävät paikkansa eivätkä sisällä tahallisia tai tahattomia virheitä. Kiistämättömyys tarkoittaa tietojärjestelmän kykyä tunnistaa ja tallentaa luotettavasti järjestelmää käyttävän henkilön tiedot. Pääsynvalvonnalla tarkoitetaan niitä menetelmiä, joilla rajoitetaan tietojenkäsittelyinfrastruktuurin käyttöä. (Hakala, Vainio & Vuorinen 2006, 4-5.)

Ihmiset ovat keskeisessä asemassa yrityksen ja organisaation toiminnassa eikä teknisillä ja fyysisillä tietoturvaratkaisuilla pelkästään voida taata hyvää tietoturvan tasoa. Jokainen tekee virheitä, mutta koulutuksella ja kokemuksen myötä virheiden määrä vähenee. Koulutus ja kokemus eivät yksistään riitä, vaan tämän lisäksi tarvitaan ohjeita, määräyksiä ja sopimuksia virheiden välttämiseksi. Heljaste ym. (2008, 24) toteavat, että mikään hallinnollinen keino ei yksistään kykene torjumaan uhkia, sillä ihminen toimii yleensä erilaisissa tilanteissa niin kuin parhaimmaksi itselleen näkee. Turvallisuustietoisuus vaikuttaa ihmisen toimintoihin normaalitilanteissa. Turvallisuustietoisuutta voidaan korottaa kouluttamalla ja tiedottamalla. Mikäli ihminen ei tiedä miksi jokin asia tehdään, hän kokee asian haittaavan omaa toimintaansa ja tällöin on vaarana, että hän laiminlyö tai keksii toisen, itselleen helpomman tavan tehdä asia. Ihmisen käyttäytymiseen vaikuttamisessa on ensiarvoisen tärkeää kertoa miksi pitää menetellä jollakin määrätyllä tavalla.

Poliisin tietoturvapolitiikan (2010) mukaan: ”Tietoturvallisuudella tarkoitetaan asiantilaa, jossa poliisin tai sen kumppaneiden tietojen, tietojärjestelmien ja tietoliikenteen saatavuuteen, eheyteen, luottamuksellisuuteen ja kiistämättömyyteen kohdistuvat uhat eivät missään

olosuhteissa aiheuta merkittävää riskiä poliisin tehokkaalle toiminnalle". VAHTI (10/2006, 10) ohjeen mukaan tietoturvallisuus on osa organisaation toiminnan laatua. Tietoturvajärjestelyjen tarkoituksena on, että tiedot, tietojärjestelmät ja palvelut on asianmukaisesti suojattu niin, että niiden luottamuksellisuuteen, eheyteen ja käytettävyyteen liittyvät riskit ovat hallinnassa.

2.1.4 Asiakirja

Asiakirjalla tarkoitetaan kirjallisen ja kuvallisen esityksen lisäksi sellaista käyttönsä vuoksi yhteen kuuluviksi tarkoitetuista merkeistä muodostuvaa, tiettyä kohdetta tai asiaa koskevaa viestiä, joka on saatavissa selville vain automaattisen tietojenkäsittelyn tai äänen- kuvantoistolaitteiden taikka muiden apuvälineiden avulla (Laki viranomaisen toiminnan julkisuudesta 1999).

Asiakirjan käsite on riippumaton siitä, minkälaiselle alustalle tai minkälaisin keinoin tieto on tallennettu. Asiakirjalla tarkoitetaan perinteisen paperimuotoisen asiakirjan lisäksi, myös sähköisesti talletettuja tietoaineistoja riippumatta niiden muodosta. (Määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

2.1.5 Viranomaisen asiakirja

Viranomaisen hallussa oleva asiakirja, jonka viranomainen tai sen palveluksessa oleva on laatinut taikka joka on toimitettu viranomaiselle asian käsittelyä varten tai muuten sen toimialaan tai tehtäviin kuuluvassa asiassa. Myös viranomaisen antaman toimeksiannon johdosta laadittu asiakirja on viranomaisen asiakirja. Viranomaiselle toimitettuna asiakirjana pidetään asiakirjaa, joka on annettu viranomaisen toimeksiannosta tai muuten sen lukuun toimivalle toimeksiantotehtävän suorittamista varten. (Määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

2.1.6 Tietoaineisto

Paperilla, sähköisillä tai muilla tietovälineillä oleva asiakirja ja tieto. Asiakirjalla tarkoitetaan Julkisuuslaissa määriteltyjä asiakirjoja.

2.1.7 Henkilötieto

Kaikenlaiset luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavat merkinnät, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi (Henkilötietolaki 1999).

2.1.8 Arkaluonteinen henkilötieto

Henkilötieto, joka kuvaa tai on tarkoitettu kuvaamaan (Henkilötietolaki 1999):

1. rotua tai etnistä alkuperää
2. henkilön yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista
3. rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta
4. henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia
5. henkilön seksuaalista suuntautumista tai käyttäytymistä
6. henkilön sosiaalihuollon tarvetta tai hänen saamiaan sosiaalihuollon palveluja, tukitoimia ja muita sosiaalihuollon etuuksia.

2.1.9 Tietoturvatasot

Tietoturvatasoilla tarkoitetaan niitä teknisiä ja hallinnollisia järjestelyjä, joiden avulla varmistetaan tietoturvallisuuden toteuttaminen eri suojaustasoilla. Perustason vaatimukset täyttävässä ympäristössä voidaan toteuttaa suurin osa viranomaisen tiedonkäsittelytarpeista. Niiden asiakirjojen käsittelyssä, jossa edellytetään korkeaa luotettavuutta kaikissa toimintaolosuhteissa ja jossa käsitellään suojaustasoa III edellyttävää luokiteltua aineistoa, viranomaisen on ylläpidettävä korotetun tietoturvatason täyttäviä rakenteita. Kriittiset ja suojaustasoille I ja II luokiteltua tietoa sisältävät tietojärjestelmät tulee toteuttaa korkean tietoturvatason ympäristöissä. (Määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

2.1.10 Salassa pidettävä asiakirja

Salassa pidettävällä asiakirjalla tarkoitetaan niitä asiakirjoja ja tietoja, jotka ovat julkisuuslain 24.1 §:n tai muun lain nojalla salassa pidettäviä. Asiakirjaa tulee käsitellä suojaustason mukaisesti ja siihen tulee tehdä suojaustason mukainen merkintä. (Määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

2.1.11 Luokiteltu asiakirja

Luokiteltu asiakirja on suojaustaso- tai turvallisuusluokiteltua tietoa sisältävä asiakirja. Salassa pidettävän tietoaineiston suojaustasoluokka määritellään sen mukaan, kuinka vakavia seurauksia tietojen oikeudettomasta paljastumisesta tai käytöstä seuraisi suojattaville eduille (Määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010).

2.1.12 Turvallisuusluokiteltava asiakirja

Salassa pidettävää tietoaineistoa sisältävä asiakirja, jonka tietojen oikeudeton paljastuminen tai käyttö voi aiheuttaa vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muille yleisille eduille julkisuuslain 24 §:n 1 momentin 2, 7 – 10 kohdissa tarkoitetulla tavalla tai asiakirja, jonka luokittelu on tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi tai asiakirja muutoin liittyy kansainväliseen yhteistyöhön. Näiden asiakirjojen käsittelyssä on noudatettava luokkaa vastaavia tietoturvavaatimuksia. (Määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

2.1.13 Suojaustasot

Suojaustasojen avulla määritellään vaatimukset, jotka tietojenkäsittely-ympäristön ja tietojen käsittelyn tulee täyttää käsiteltäessä luokiteltavaa asiakirjaa. Suojaustasot toteutetaan neliportaisen luokitusjärjestelmän avulla. Kullekin suojaustasolle on asetettu omat tekniset ja toiminnalliset vaatimukset. Näiden menettelyjen avulla turvataan salassa pidettävän ja muun luokittelua edellyttävän tiedon asianmukainen käsittely (tietoturvallisuusasetus, 9 §). Tietojen käsittely tapahtuu suojaustason mukaisesti riippumatta siitä onko kysymyksessä suojaustaso- vai turvallisuusluokiteltu tieto. (Määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

2.2 Kehittämistyössä sovelletut keskeiset viitekehykset

Poliisitoiminta perustuu voimassa oleviin lakeihin ja asetuksiin ja siksi myös tietoturvallisuuteen liittyvät viitekehykset pohjautuvat lakeihin ja asetuksiin.

2.2.1 Laki viranomaisen toiminnan julkisuudesta (621/1999)

Lain viranomaisen toiminnan julkisuudesta (Julkisuuslaki) mukaan viranomaisen asiakirjat ovat julkisia, jollei lailla erikseen toisin säädetä. Laissa säädetään mm. oikeudesta saada tietoa viranomaisten asiakirjoista sekä viranomaisten asiakirjojen salassapidosta ja muista rajoituksista ja viranomaisten velvollisuuksista tämän lain toteuttamiseksi. Lain tarkoituksena on toteuttaa avoimuutta ja hyvää tiedonhallintatapaa viranomaisten toiminnassa sekä antaa mahdollisuus valvoa ja vaikuttaa julkisen vallan käyttöön. Laki on yksi keskeisimmistä viranomaisen tietoturvallisuuteen liittyvistä laeista.

2.2.2 Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010)

Asetuksessa säädetään viranomaisten asiakirjojen käsittelyä koskevista yleisistä tietoturvallisuusvaatimuksista sekä asiakirjojen luokittelun perusteista. Tietoturva-asetus astui voimaan 1.10.2010 ja sen mukaan jokaisen valtionhallinnon organisaation tulee toteuttaa tietoturvallisuuden perustaso 1.10.2013 mennessä ja korkeampi tietoturvallisuuden taso 1.10.2015 mennessä, jos organisaatiossa luokitellaan asiakirjoja ja käsitellään korkeampaa kuin IV suojaustason tietoaineistoja. Eri tasojen vaatimuksia käsitellään myöhemmin tässä raportissa.

2.2.3 Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (Vahti 2/2010)

Ohjeen tavoitteena on tehostaa ja yhdenmukaistaa lain viranomaisen toiminnan julkisuudesta (621/1999) perusteella 1.10.2010 voimaantulleen tietoturvallisuusasetuksen (681/2010) täytäntöönpanoa. Ohjeen avulla viranomaisessa voidaan saavuttaa asetuksen mukainen tietoturvataso. Ohje on tarkoitettu koko organisaation henkilöstön käyttöön ja organisaatioiden tulee toiminnassaan ottaa huomioon ohjeessa kuvatut linjaukset.

2.2.4 Poliisihallituksen määräys poliisin tietoturvapolitiikasta (2020/2010/4157)

Poliisihallituksen määräyksen poliisin tietoturvapolitiikasta (2010) mukaan poliisihallinnossa noudatetaan Poliisihallituksen antamia tietoturvallisuuden määräyksiä ja ohjeita. Yksiköillä on mahdollisuus antaa tarkentavia sisäisiä määräyksiä ja ohjeita. Määräyksissä ja ohjeissa huomioidaan sisäasiainhallinnon tietoturvamääräykset sekä soveltuvin osin valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI ohjeet. (Poliisihallituksen määräys poliisin tietoturvapolitiikasta 2010.)

Poliisihallituksen määräys poliisin tietoturvapolitiikasta on poliisin ylimmän johdon kannanotto, joka määrittelee tietojen turvaamisen tavoitteet, vastuut ja toteutuskeinot poliisihallinnossa. Tietoturvapolitiikkaa tarkennetaan erillisissä määräyksissä ja ohjeissa.
(Poliisihallituksen määräys poliisin tietoturvapolitiikasta 2010.)

<u>Tietoturvatoiminnan tavoitteet poliisissa</u>

Poliisihallituksen määräyksen mukaan:
”Poliisin tietoturvallisuuden lähtökohtana on toiminnan jatkuvuuden varmistaminen normaali- ja häiriötilanteessa sekä poikkeusoloissa. Lähtökohtana on myös poliisin sekä sen yhteistyökumppaneiden tietojen luotettava, sopimusten ja lainmukainen käsittely riippumatta tiedon olomuodosta.” (Poliisihallituksen määräys poliisin tietoturvapolitiikasta 2010.)

Henkilötietoja käsitellään olemassa olevien lakien mukaisesti ja yksityisyyden suojaa kunnioittaen ja tietoturvatyön keskeinen tavoite on osaltaan poliisin luotettavan maineen turvaaminen yhteiskunnan kaikilla tasoilla (Poliisihallituksen määräys poliisin tietoturvapolitiikasta 2010).

Pyrkimyksenä on myös toimia aina vähintään Valtioneuvoston asetuksen tietoturvallisuudesta valtionhallinnossa (681/2010) määrittelemällä korotetulla tasolla. Yleisenä tavoitteena on kansallisesti ja kansainvälisesti korkeatasoinen tietoturvallisuuden hallinta. (Poliisihallituksen määräys poliisin tietoturvapolitiikasta 2010.)

Tietoturvatoiminnan organisointi, vastuut ja tehtäväjako

Poliisin tietoturvallisuuden organisaatiota ja vastuita käsitellään Poliisihallituksen määräyksessä tietoturvapolitiikasta (2010) sekä vuonna 2008 annetussa SM:n Poliisiosaston määräyksessä poliisihallinnon tietoturvaperiaatteista. Koska SM:n määräys poliisihallinnon tietoturvaperiaatteista on annettu ennen poliisin laajaa rakenneuudistusta, jonka viimeisessä vaiheessa perustettiin Poliisihallitus vuoden 2010 alusta, sisältää SM:n määräys ainakin joiltain osin vanhentunutta tietoa tietoturvallisuuden organisaation ja vastuiden osalta. SM:n määräyksessä poliisihallinnon tietoturvaperiaatteissa määritellään tietoturvapolitiikkaa tarkemmin tietoturvallisuuden vastuista eri tasoilla.

Poliisihallituksen määräyksen mukaan poliisin tietoturvallisuutta johtaa poliisiylijohtaja ja Poliisihallitukseen sijoitettu (SM:n määräyksessä Poliisin ylijohdossa työskentelevä) poliisin tietoturvapäällikkö vastaa poliisihallinnon tietoturvallisuustoiminnan ja tietosuojan ohjaamisesta, valvonnasta, kehittämisestä ja yhteensovittamisesta sekä poliisin ylimmän johdon raportoinnista. Tietoturvallisuus kuuluu yhtenä osana poliisin organisaatioturvallisuuteen. (Poliisihallituksen määräys poliisin tietoturvapolitiikasta 2010.)

Poliisihallinnossa toimii tietoturvatyöryhmä, jonka tehtävänä on tukea tietoturvallisuuden kehitystä ja tietoturvatoiminnan seuraamista. Vastuu tietoturvallisuudesta, tietoturvatietoisuudesta ja asenteiden kehittämisestä ohjeistuksella, koulutuksella, valvonnalla, tarkastuksilla sekä omalla esimerkillä kuuluu poliisiyksiköiden johdolle. Tietoturvatyön johtaminen on osa normaalia johtamis- ja tulosohjausprosessia. Poliisiyksiköt nimeävät yksikön tietoturvapäällikön tai tietoturvavastaavan tai jos nimeämistä ei tehdä, tietoturvapäällikön tehtäviä hoitaa yksikön turvallisuuspäällikkö. Tietoturvapäällikön ja -vastaavan tehtävänä on kehittää ja ylläpitää tietoturvallisuutta, tietoturvatoimintaa, tietoturvallisuuden tilannekuvaa sekä oikeiden käytäntöjen ja asenteiden omaksumista. (SM 2008.) Lisäksi yksiköiden tietoturvapäälliköiden

ja tietoturvavastaavien tulee järjestää aktiivisesti tietoturvakoulutusta. Poliisiyksiköt voivat nimetä myös sisäisiä turvallisuus- tai tietoturvaryhmiä tukemaan tietoturvatyötä. (Poliisihallituksen määräys poliisin tietoturvapolitiikasta 2010.)

Esimiesten tehtävänä on alaisten tukeminen ja ohjaaminen sekä sen varmistaminen, että heidän vastuualueeseensa sisältyvät tietoturvamenettelyt suoritetaan asianmukaisesti. Esimiehen tehtävänä on määritellä alaisensa tarvitsemat käyttöoikeudet erilaisiin tietojärjestelmiin ja tietoihin sekä esimiehen tehtävänä on pitää huoli tarpeettomien käyttöoikeuksien poistamisesta. (SM:n Poliisiosaston määräys poliisihallinnon tietoruvaperiaatteista 2008).

Jokaisen poliisihallinnon palveluksessa olevan henkilön sekä jokaisen poliisin tietoja käsittelevän tulee noudattaa annettuja määräyksiä, ohjeita sekä toiminta- ja työskentelytapoja sekä tulee raportoida havaitsemistaan mahdollisista tietoturvallisuuden puutteista, väärinkäytöksistä tai epäilemistään tietoturvarikkomuksista yksikön tietoturvapäällikölle tai -vastaavalle. Tietoturvapolitiikka sekä sitä tukevat määräykset ja ohjeet annetaan tiedoksi koko henkilöstölle ja heidän tulee toimia niiden mukaisesti. Jokaisen poliisihallinnon palveluksessa olevan henkilön on käytävä tietoturvakoulutus määräajoin.
(Poliisihallituksen määräys poliisin tietoturvapolitiikasta 2010.)

2.2.5 SM:n Poliisiosaston määräys poliisihallinnon tietoturvaperiaatteista (SMDno/2008/353)

Tietoturvaperiaatteiden tarkoituksena on tarkentaa tietoturvapolitiikassa määriteltyjä linjauksia. Tietoturvaperiaatteet sisältävät pääasiassa ns. yleiset kontrollit eli kaikille yhteiset tietoturvajärjestelyt. Periaatteiden avulla luodaan puitteet tietoturvalliselle toiminnalle.

Sisäasianministeriön Poliisiosaston määräys Poliisihallinnon tietoturvaperiaatteet (SMDno/2008/353) on annettu ennen nykyisen Poliisihallituksen perustamista vuoden 2010 alussa, joten sen sisältö on joiltain osin vanhentunutta ja osin uudemmalla määräyksellä kumottua (Poliisihallituksen määräys (2020/2010/4030) poliisin salassa pidettävien tietoaineistojen käsittelystä).

2.2.6 Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä (2020/2010/4030)

Poliisihallituksen määräys (2020/2010/4030) poliisin salassa pidettävien tietoaineistojen käsittelystä sisältää salassa pidettävien tietoaineistojen käsittelyssä noudatettavat periaatteet poliisihallinnossa. Määräys perustuu lakiin viranomaisen toiminnan julkisuudesta (621/1999) sekä 1.10.2010 voimaan tulleeseen Valtioneuvoston asetukseen tietoturvallisuudesta valtionhallinnossa (681/2010). Määräyksen laatimisessa on otettu huomioon sisäasiainhallinnon voimassa oleva ohjeistus sekä Ohje tietoturvallisuudesta annetun asetuksen täytäntöönpanosta. (Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Määräys kumoaa SM:n määräyksen Poliisihallinnon tietoturvaperiaatteet (SMDno/2008/353) kappaleiden Tietoaineistoturvallisuus, Tietoaineiston määritelmä sekä yhdistelmä salassa pidettävän tietoaineiston käsittelystä poliisissa osalta.

Lainsäädäntö ja velvoitteet

Salassa pidettävän aineiston käsittelyssä on noudatettava erityistä huolellisuutta. Virkamiehen ja julkisyhteisön työntekijän salassapitovelvollisuuden rikkomisesta ja muiden henkilöiden salassapitorikoksesta ja rikkomuksesta säädetään rikoslaissa.
(Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Julkisuuslain mukaan viranomaisen asiakirjat ovat julkisia, jollei lailla toisin säädetä. Asiakirjan käsite on julkisuuslaissa laaja ja se kattaa myös erilaiset tekniset tallenteet. Laissa on erikseen määritelty ne asiakirjat, jotka ovat joko kokonaan tai osittain salassa pidettäviä. Salassapitovelvollisuudesta on säännöksiä myös muissa laeissa. Henkilötietojen käsittelyä koskevat yleissäännökset sisältyvät henkilötietolakiin (523/1999). Sen sijaan viranomaisten henkilörekisterien julkisuutta ja salassa pitoa arvioidaan julkisuuslain ja mahdollisten erityislakien mukaisesti. Sellaisiin muistiinpanoihin ja luonnoksiin, jotka muuten jäävät julkisuuslain mukaan viranomaisen asiakirjan käsitteen ulkopuolelle, sovelletaan kuitenkin lain salassapitosäännöksiä. (Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Julkisuuslain mukaan jokaisen asiakirjan julkisuus on selvitettävä tapauskohtaisesti silloin, kun joku pyytää asiakirjaa nähtäväkseen tai saadakseen siitä kopion. Salassapitoa ei saa kuitenkaan ulottaa laajemmalle kuin suojattava etu vaatii. Jos asiakirjasta vain osa on salassa pidettävää, on viranomaisen annettava asiakirjasta tieto muilta osin. Kieltäytyessään antamasta tietoa asiakirjasta, on viranomaisen tehtävä päätös asetetussa määräajassa sekä perusteltava päätöksensä. Tietoturvallisuuden varmistamiseksi tehtävä asiakirjojen luokittelu ja

sitä vastaavien merkintöjen tekeminen asiakirjaan ei poista velvollisuutta arvioida asiakirjan julkisuus erikseen ja tapauskohtaisesti silloin, kun viranomaiselta pyydetään asiakirjaa. Kansainvälisistä tietoturvallisuusvelvoitteista ja turvallisuusluokitusmerkinnöistä säädetään erikseen. (Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Lain mukaan tietoa salassa pidettävän asiakirjan sisällöstä saa antaa vain viranomainen tai se virkamies, jolle tällainen oikeus on nimenomaisesti työjärjestyksessä tai vastaavalla tavalla annettu. Salassa pidettävän tiedon luovuttaminen ilman asianmukaista oikeutta on rangaistavaa. (Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Luokittelun perusteet

Julkisuuslaki asettaa viranomaiselle velvoitteet hallita käytössään olevia tietoaineistoja hyvän tiedonhallintatavan mukaisesti. Tietoaineistojen käytettävyyttä, eheyttä ja luottamuksellisuutta hallitaan luokittelemalla aineisto eri luokkiin tiedolle asetettujen toiminnallisten vaatimusten pohjalta. (Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Julkisuuslainsäädännön ja salassapitosäännösten pohjalta määritetään onko tietoaineiston sisältämä tieto julkista vai salassa pidettävää. Salassa pidettävän tietoaineiston käsittelyä ohjataan suojausluokkien avulla ja niitä käsitellään kyseistä tietoa vastaavan suojaustason edellyttämällä tasolla. Suojausluokka määritellään sen mukaan, kuinka vakavia seurauksia tietojen oikeudettomasta paljastumisesta tai käytöstä seuraisi suojattavalle edulle. Seuraukset on arvioitava konkreettisesti ja ottaen huomioon suojattava etu kokonaisuutena. (Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Tietoturva-asetuksessa on määritelty ne muut asiakirjat, jotka voidaan luokitella suojaustasoa IV edellyttäväksi asiakirjaksi. Tällaisia ovat vain sellaiset asiakirjat ja tiedot, joiden luovuttaminen on lain mukaan viranomaisen harkinnassa tai joita saadaan lain mukaan luovuttaa vain määrättyyn tarkoitukseen. Lisäksi tiedon oikeudettoman paljastumisen tulee voida aiheuttaa haittaa yleiselle tai yksityiselle edulle tai heikentää viranomaisen toimintaedellytyksiä. (Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Salassapidon arviointi tulee tehdä jo asiakirjaa laadittaessa. Luokitusmerkinnän tekemisestä asiakirjaan päättää asiakirjan allekirjoittaja tai työjärjestyksessä erikseen määrätty henkilö ja se kertoo laatijan ja allekirjoittajan käsityksen siitä, millä tavalla asiakirja on suojattava ja kenelle se on tarkoitettu. Asiakirjan sisältämän salassa pidettävän tiedon paljastaminen sivullisille ei ole sallittua, vaikka asiakirjaan ei olisi merkitty suojaustasoa.

Sellainen salassa pidettävä tietoaineisto, jonka tietojen oikeudeton paljastuminen tai käyttö voi aiheuttaa vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muille yleisille eduille julkisuuslain 24§:n 1 mom. 2,7-10 kohdissa tarkoitetulla tavalla, on turvallisuusluokiteltava. (Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Salassapitomerkinnät

Salassapitomerkintä on tehtävä viranomaisen asiakirjaan, joka annetaan asianosaiselle ja joka on salassa pidettävä toisen tai yleisen edun vuoksi. Merkintä on suositeltavaa tehdä myös salassa pidettävään asiakirjaan, joka annetaan toiselle viranomaiselle tai sille, joka viranomaisen toimeksiannon perusteella käsittelee salassa pidettäviä tietoja.
(Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Salassapitomerkintä tehdään pääsääntöisesti asiakirjan ensimmäiselle sivulle oikeaan yläkulmaan. Merkinnästä tulee käydä ilmi, miltä osin asiakirja on salassa pidettävä ja mihin salassapito perustuu sekä mille suojaustasolle tietoaineisto luokitellaan.
(Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Suojaustasot ja merkinnät

SALASSA PIDETTÄVÄ (suojaustaso I – IV) –merkintää käytetään asiakirjoissa, jotka sisältävät joko julkisuuslain 24.1§:n 1, 3-6 sekä 11 -32 tai muussa laissa määriteltyä salassa pidettävää tietoa. Tämän lisäksi leimaa voidaan käyttää suojaustasolla IV asiakirjoihin, joiden luovuttaminen on viranomaisen harkinnassa tai joita saadaan lain mukaan luovuttaa vain määrättyyn tarkoitukseen ja tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa haittaa yleiselle tai yksityiselle edulle tai heikentää viranomaisen toimintaedellytyksiä.
(Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Suojaustasot ovat:

- suojaustaso I (ST I), jos salassa pidettävän tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa erityisen suurta vahinkoa salassapitosäännöksessä tarkoitetuille yleisille eduille;
- suojaustaso II (ST II), jos salassa pidettävän tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa merkittävää vahinkoa salassapitosäännöksessä tarkoitetuille yleisille eduille;
- suojaustaso III (ST III), jos salassa pidettävän tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitetulle yleisille tai yksityisille eduille ja oikeuksille;

- suojaustaso IV (ST IV), jos salassa pidettävän tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa haittaa salassapitosäännöksessä tarkoitetuille yleisille tai yksityisille eduille tai, jos tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa haittaa yleiselle tai yksityiselle edulle tai heikentää viranomaisen toimintaedellytyksiä.

(Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

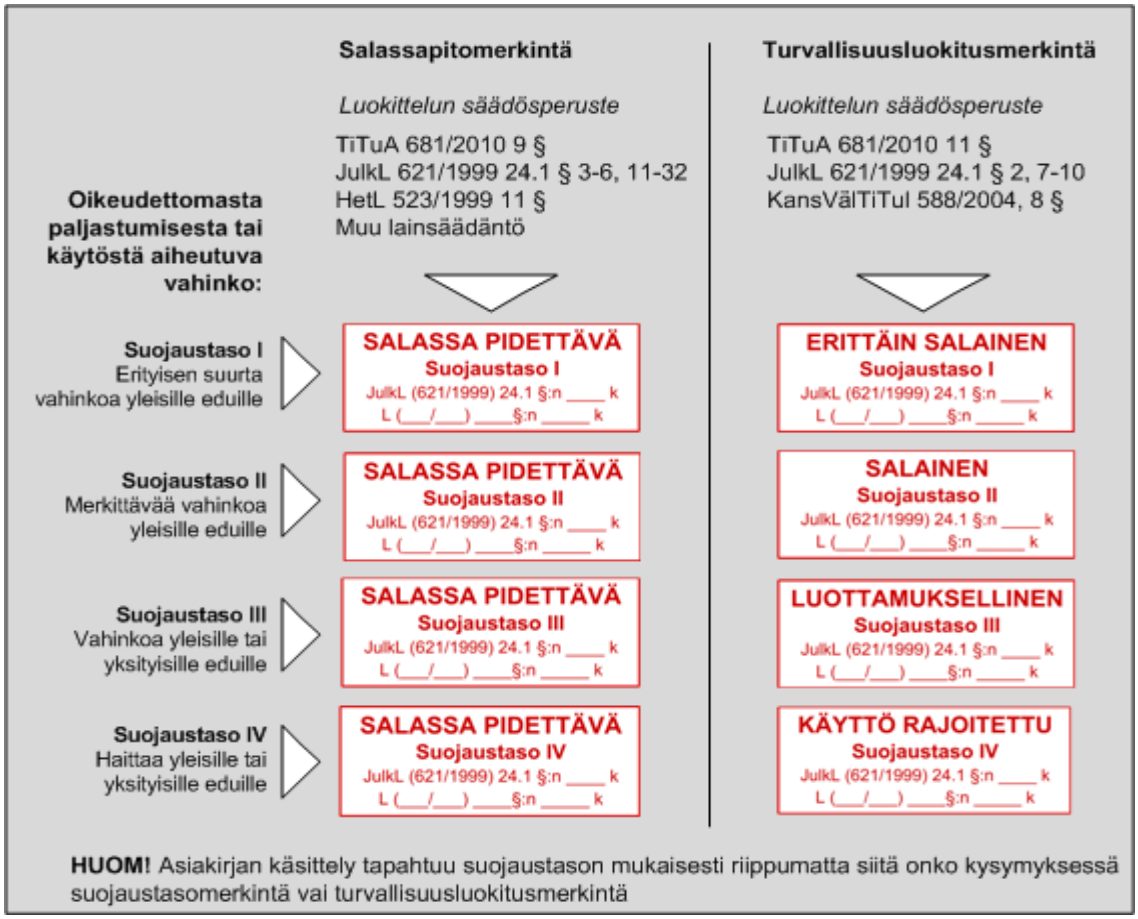
Luokitusmerkintä voidaan jättää tekemättä, jos kaikki asiakirjaa viranomaisessa käsittelevät ovat tietoisia asiakirjan salassapidosta ja sen käsittelyssä noudatettavista menettelytavoista (Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010).

Turvallisuusluokat ja merkinnät

Tietoaineistoa voidaan turvallisuusluokitella tietoturva-asetuksessa osoitetuissa tapauksissa neljään turvallisuusluokkaan. Merkintää ei saa käyttää muissa kuin julkisuuslain 24§ 1 mom. 2, 7 -10 kohtiin tarkoitetuissa tapauksissa sekä kv. tietoturvavelvoitteen toteuttamiseksi tai jos asiakirja muutoin liittyy kv. yhteistyöhön. (Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Turvallisuusluokat ovat:

- Turvallisuusluokka I (ERITTÄIN SALAINEN), jos salassa pidettävän tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa erityisen suurta vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muille julkisuuslain 24 § 1 mom. 2,7 – 10 kohdassa tarkoitetuille yleisille eduille;
- Turvallisuusluokka II (SALAINEN), jos salassa pidettävän tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa merkittävää vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muille julkisuuslain 24 § 1 mom. 2,7 – 10 kohdassa tarkoitetuille yleisille eduille;
- Turvallisuusluokka III (LUOTTAMUKSELLINEN), jos salassa pidettävän tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muille julkisuuslain 24 § 1 mom. 2,7 – 10 kohdassa tarkoitetuille yleisille eduille;
- Turvallisuusluokka IV (KÄYTTÖ RAJOITETTU), jos salassa pidettävän tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa haittaa julkisuuslain 24 § 1 mom. 2,7 – 10 kohdassa tarkoitetuille yleisille eduille.
  (Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)



Kuvio 2: Tietoaineistojen suojaustasot ja luokitusmerkinnät (POHA 2020/2010/4030)

Henkilötietojen luokitus ja merkinnät

Henkilötietojen käsittelyä ja henkilörekistereitä ohjaavat julkisuuslain lisäksi henkilötietolaki, laki henkilötietojen käsittelystä poliisitoimessa (761/2003) ja useat eri henkilötietojen käsittelyä koskevat erityislait. Poliisin henkilörekistereiden ja niihin sisältyvien tietojen julkisuus- ja salassapitoperusteet sekä luokitusta koskevat vaatimukset ovat samoja kuin muissakin asiakirjoissa. (Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Arkaluonteisia henkilötietoja sisältävät asiakirjat luokitellaan pääsääntöisesti suojaustasolle III. Muita kuin arkaluonteisia henkilötietoja sisältävät asiakirjat luokitellaan suojaustasolle IV, mikäli se on suojattavan edun vuoksi tarpeen. Myös henkilötietoja sisältäviä luokittelemattomia asiakirjoja käsitellään lähtökohtaisesti suojaustason IV mukaisesti. Henkilötunnuksen sisältäviä asiakirjoja on käsiteltävä suojaustason IV mukaisesti, ellei asiakirjan sisällön perusteella asiakirjaa kuulu käsitellä korkeamman suojaustason vaatimuksen mukaisesti. (Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Tietoaineistojen käsittelyvaatimukset

Tietoaineiston hallussapito- ja käsittelyoikeudet

I ja II suojaustason tietoaineistoa saavat käsitellä vain vastaanottajaksi merkityt henkilöt, jotka ovat siihen oikeutettuja sekä henkilöt, jotka ovat oikeutettuja tällaisen tietoaineiston tekniseen hallussapitoon ja käsittelyyn. Käyttöoikeus I ja II suojaustasoon luokiteltuun tietoaineistojen käyttöön voidaan antaa ainoastaan henkilöille, joilla työtehtäviensä vuoksi on tarve saada tietoja tietoaineistosta tai muutoin käsitellä sitä. Poliisin yksiköiden on pidettävä ajantasaista luetteloa niistä työtehtävistä, joissa on oikeus käsitellä suojaustasoa I ja II edellyttäviä asiakirjoja. Kuten huomataan, on I ja II suojaustasoon luokiteltujen tietojen käsittelyn ja käytön käyttöoikeudet rajattu hyvin pienelle joukolle poliisihallinnon työntekijöitä, kuten esim. poliisipäällikkö ja apulaispoliisipäällikkö. Lisäksi I ja II suojaustason tietoaineiston käsittelyyn varattaville laitteistoille ja säilyttämiseen vaadittaville tiloille sekä tietoaineiston käsittelylle on asetettu erityisiä hyvin korkeita vaatimuksia.
(Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

III ja IV suojaustasojen tietoaineistoa voivat pitää hallussaan ja käsitellä kaikki poliisihallinnon virkamiehet ja työntekijät heidän työtehtäviensä mukaisissa asioissa (Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010).

Tietoaineiston käsittely, tallennus tietovälineille sekä kopiointi ja tulostus

I suojaustason tietoaineiston käsittelyä varten on varattava erilliset vain tätä tarkoitusta varten tarkoitetut laitteet, jotka ovat erillään tietoverkosta. I ja II suojaustason tietoaineiston käsittely vaatii tilat, joihin on pääsy vain tunnistetuille henkilöille ja aineiston tallennus on sallittua vain kun kyseinen tieto tai koko tietovälineen sisältö on vahvasti salattu. I ja II suojaustason tietoaineiston tulostus tapahtuu laitekohtaisella oheistulostimella ja tulosteet on numeroitava ja niiden jakelu tulee merkitä alkuperäiseen asiakirjaan tai erilliseen jakoluetteloon. (Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

III ja IV suojaustason tietoaineistoa saa käsitellä ja tallentaa tietoverkkoon kytketyllä korotetun tietoturvatason vaatimukset täyttävillä tietojärjestelmillä. Tietoaineistoa saa tulostaa verkkotulostimella vain sillä edellytyksellä, että tulostettu asiakirja noudetaan välittömästi tulostimelta. III ja IV suojaustason aineistot on tallennettava tietojärjestelmiin, levyalueille tai erillisille tietovälineille siten, että tietoa voivat käsitellä vain siihen oikeutetut henkilöt. Tallennus siirrettäville tietovälineille, kuten esim. USB muistitikulle, tulee tehdä aina vahvasti salattuna. (Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Tietoaineiston säilytys

I suojaustason asiakirjat kirjataan erittäin salaisten asioiden diaariin ja II suojaustason asiakirjat salaisten asioiden diaariin. I ja II suojaustason paperiasiakirjat, niiden luonnokset sekä niitä sisältävät tietovälineet on säilytettävä ja arkistoitava holvissa tai murtosuojatussa säilytyskaapissa tai vastaavassa ja niiden arkistoille on määrättävä omat vastuulliset hoitajansa (Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Pääsy arkistoihin, tietokonesaleihin tai muihin tietojärjestelmien ylläpidon tai tietoliikenteen toimivuuden kannalta merkityksellisiin tiloihin, joissa säilytetään tai käsitellään suojaustasoon III kuuluvia asiakirjoja tai suojaustasoon IV kuuluvia valtakunnalliseen henkilörekisteriin talletettuja asiakirjoja, tulee rajata vain tunnistettaviin henkilöihin (Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010).

Suojaustasoon III ja IV kuuluvat asiakirjat kirjataan julkisten asioiden diaariin siten että tietoihin ja asiakirjoihin on rajattu pääsy. Tietoaineistojen diaaritiedot ja otsikoinnit on laadittava siten, etteivät ne itsessään sisällä III tai IV suojaustason tietoa. III ja IV suojaustasoon kuuluvista tietoaineistojen laatimisesta, lähettämisestä ja vastaanottamisesta on pidettävä luetteloa myös sellaisissa toimipisteissä, joissa ei ole muodostettua omaa diaaria. Paperisia asiakirjoja tulee säilyttää lukitussa kaapissa tai vastaavassa.
(Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Tietoaineiston kuljettaminen virkapaikan ulkopuolelle ja käsittely

I suojaustason tietoaineistoa tai niitä sisältäviä tietovälineitä ja II suojaustason paperisia tai laajoja sähköisiä tietoaineistoja ei saa viedä virkapaikan ulkopuolelle ilman yksikön päällikön erillistä päätöstä. Päätöksistä pitää kirjaa yksikön tietoturvapäällikkö tai -vastaava. II suojaustason tietoaineistoa tai niitä sisältäviä tietovälineitä saa kuljettaa virkapaikan ulkopuolelle käsittelyyn oikeutettu henkilö vain välttämättömiin työtehtäviin liittyen. Tietovälineelle tallennetun tietoaineiston tulee olla vahvasti salattu. Suojaustasoon I ja II kuuluvaa tietoaineistoa ei saa käsitellä poliisin toimipisteen ulkopuolella ellei kyseessä ole sisäasiainhallinnon tai muun turvallisuusviranomaisen I tai II suojaustasoon luokitellut tilat. Yksikön päällikön päätöksellä voidaan suojaustasoon II kuuluvia tietoaineistoja käsitellä poliisin toimitilojen ulkopuolella. Poliisin ja hallinnonalan tietotekniseen ympäristöön tallennettujen I ja II suojaustasoihin kuuluvien tietoaineistojen etäkäyttö on kielletty.
(Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

III ja IV suojaustasoon kuuluvaa tietoaineistoa saa kuljettaa virkapaikan ulkopuolelle työtehtäviin liittyen ja tietovälineelle tallennettua aineistoa vain jos tallennettu tietoaineisto on vahvasti salattu. Suojaustasoon III ja IV kuuluvien tietoaineistojen käsittely poliisin toimipisteiden ulkopuolella on mahdollista työtehtäviin liittyen, ottaen kuitenkin huomioon velvoit-

teet salassa pidettävän tiedon käsittelystä ja suojaamattomasta ympäristöstä aiheutuvat erityiset riskit kuten salakuuntelu tai salakatselun mahdollisuus. Neuvottelutiloista ja vastaavista on poistettava salassa pidettävää tietoaineistoa sisältävät materiaalit ja piirrokset viimeistään tilaisuuden päätyttyä.
(Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Tietoaineiston toimittaminen vastaanottajalle
I suojaustason tietoaineiston vastaanottaja on aina henkilö. Tietoaineistoa voidaan lähettää vain kuriirin välityksellä ja vastaanottaminen tulee aina varmentaa. Aineisto pakataan sinetöityyn mustaan läpinäkymättömään kirjekuoreen ja sen jälkeen tavalliseen kirjekuoreen tai tähän tarkoitukseen valmistettuun tietoaineistopussiin. Missään tapauksessa ei I suojaustasoon kuuluvaa tietoaineistoa saa lähettää sähköisessä tietoverkossa.
(Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

II suojaustason tietoaineiston vastaanottaja voi olla henkilö tai organisaatio. Aineistoa voidaan lähettää vastaanottajalle vahvasti salattuna sähköisen tietojärjestelmän tai tietoverkon välityksellä. Sähköisessä muodossa esim. postin tai kuriirin välityksellä lähetettävä materiaali tulee tallentaa käyttämättömälle tietovälineelle ja salata vahvasti. II suojaustason paperinen tietoaineisto voidaan lähettää kirjattuna kirjeenä ja aineisto tulee pakata sinetöityyn mustaan läpinäkymättömään kirjekuoreen joka pakataan tavalliseen kirjekuoreen. Mustan kirjekuoren sijasta voidaan käyttää myös tähän tarkoitukseen valmistettua tietoaineistopussia.
(Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

III suojaustason tietoaineiston vastaanottaja voi olla henkilö tai organisaatio ja tietoaineistoa saa lähettää vastaanottajalle vahvasti salattuna sähköisen tietojärjestelmän tai tietoverkon välityksellä. III suojaustason tietoaineistoa voidaan myös lähettää vastaanottajalle manuaalilähetyksenä. Sähköisessä muodossa tallennetut manuaalilähetykset on vahvasti salattava. Lähetys tulee tapahtua läpinäkymättömässä kirjekuoressa ja se suositellaan lähetettäväksi kirjattuna kirjeenä.
(Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

IV suojaustason tietoaineiston vastaanottaja voi olla henkilö tai organisaatio ja tietoaineistoa saa lähettää sisäasiainministeriön hallinnonalan yhteisessä tietoliikenneverkossa salaamattomassa muodossa sähköisesti. Hallinnonalan ulkopuolelle lähetettäessä pitää tietoaineisto vahvasti salata. Tietoaineistoa voidaan lähettää myös telekopiosanomana vastaanottaja varmistaen. Lisäksi tietoaineistoa voidaan lähettää vastaanottajalle manuaalilähetyksenä, normaalin postin mukana suljetussa läpinäkymättömässä kirjekuoressa. Sähköisessä muodossa tallennetut manuaalilähetykset on vahvasti salattava. (Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Tietoaineistojen hävittäminen

I ja II suojaustasoihin luokitellun aineiston hävittämisestä on tehtävä merkintä diaariin. I ja II suojaustason paperiset aineistot hävitetään silppuamalla ne suojaustasovaatimuksen mukaisella silppurilla tehtävään määrätyn henkilön toimesta.
(Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Tarpeettomaksi tullut tietoaineisto hävitetään arkistonmuodostussuunnitelman mukaisesti. III ja IV suojaustasoihin luokitellut paperiset tietoaineistot tuhotaan silppuamalla tai keräämällä ne lukittaviin paperinkeräysastioihin.
(Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Hävitettävät, salassa pidettävää tietoa sisältäneet tai sisältävät muistivälineet kuten CD- ja DVD –levyt, magneettinauhat, kasetit, muistitikut sekä –kortit toimitetaan lukittaviin säilytysastioihin ja niiden fyysinen tuhoaminen tapahtuu poliisihallinnon voimassa olevien sopimusten mukaisesti.
(Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Käytöstä poistettavat tai huollettavat tietokoneet, älypuhelimet ja muut mahdollisesti kierrätettävät, tietoa sisältäneet laitteet tai niiden massamuistit toimitetaan yksikössä laitteita koordinoivalle taholle. Laitteiden massamuistien turvallinen tyhjennys toteutetaan poliisin tai Haltikin henkilöstön toimesta ennen luovuttamista ulkopuoliselle taholle. Mikäli tietokoneilla, älypuhelimilla tai muilla kierrätettävillä laitteilla on käsitelty tai tallennettu salassa pidettävää tietoa, tulee turvallinen tyhjennys tehdä myös ennen siirtoa toiselle käyttäjälle, ellei kyseessä ole yhteiskäyttöön määritellystä laitteesta. Salassa pidettävää tietoa sisältäneitä siirrettäviä muistivälineitä ei lähtökohtaisesti luovuteta eteenpäin.
(Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Silppurit ja keräysastiat on merkittävä niillä tuhottavan tai niihin sijoitettavan tietoaineiston suojaustason mukaisesti ja ne on sijoitettava suojausluokan edellyttämään tilaan. Seuraavalla sivulla taulukkoon 2 on koottu poliisin salassa pidettävien tietoaineistojen käsittely suojaustasojen mukaan.
(Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Käsittely	Suojaustaso			
	IV	III	II	I
Käsittely, laatiminen				
Tietoverkosta erillään oleva poliisihallinnon työasema	Kyllä	Kyllä	Kyllä	Kyllä
Tietoverkkoon kytketty poliisihallinnon työasema	Kyllä	Kyllä	Kyllä	Ei
Poliisihallinnon mobiililaitteet	Kyllä	Kyllä	Ei	Ei
Etäkäyttö	Kyllä	Kyllä	Ei	Ei
Tulostus ja kopiointi				
Verkkotulostin tai verkkoon kytketty monitoimilaite	Kyllä	Kyllä	Ei	Ei
Verkosta erillään oleva tulostin tai monitoimilaite	Kyllä	Kyllä	Kyllä	Kyllä
Kirjaaminen				
Julkinen diaari	Kyllä	Kyllä	Ei	Ei
Salaisten asiakirjojen diaari	Ei	Ei	Kyllä	Ei
Erittäin salaisten asiakirjojen diaari	Ei	Ei	Ei	Kyllä
Lähettäminen				
Kirjaamaton kirje	Kyllä	Ei	Ei	Ei
Kirjattu kirje, huomioitava ST II erityisvaatimukset	Kyllä	Kyllä	Kyllä	Ei
Kuriiriposti, huomioitava ST I ja II erityisvaatimukset	Kyllä	Kyllä	Kyllä	Kyllä
Salaamattomana sähköpostina poliisihallinnon ulkopuolelle	Ei	Ei	Ei	Ei
Salaamattomana sähköpostina poliisihallinnon sisällä	Kyllä	Ei	Ei	Ei
Salattuna sähköpostina	Kyllä	Kyllä	Kyllä	Ei
Fax, vastaanottaja varmistettu	Kyllä	Ei	Ei	Ei
Säilyttäminen, tallentaminen				
Murtosuojattu tila, kuten kassakaappi tai holvi	Kyllä	Kyllä	Kyllä	Kyllä
Lukittu kaappi tai muu vastaava tila	Kyllä	Kyllä	Ei	Ei
Tietoverkkoon kytketty poliisihallinnon työasema	Kyllä	Kyllä	Kyllä	Ei
Tietoverkosta erillään oleva poliisihallinnon työasema	Kyllä	Kyllä	Kyllä	Kyllä
Poliisihallinnon salatut tallennusmediat ja muistilaitteet	Kyllä	Kyllä	Kyllä	Kyllä
Poliisihallinnon mobiililaitteet	Kyllä	Kyllä	Ei	Ei
Hävittäminen				
Paperinkeräys	Ei	Ei	Ei	Ei
Lukittu tietosuojalaatikko ja ulkoisten medioiden lukitut keräyslaatikot	Kyllä	Kyllä	Ei	Ei
Silppuri, huom. silppurin luokitus (taso merkittävä)	Kyllä	Kyllä	Kyllä	Kyllä

Taulukko 2: Poliisin salassa pidettävien tietoaineistojen käsittely (Määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

Tiedon antaminen salassa pidettävästä tietoaineistosta
Suojaustaso ei sellaisenaan luo vielä salassapitovelvollisuutta ja viranomaisen on arvioitava asiakirjan julkisuus aina erikseen, kun tietoaineistosta pyydetään tietoa. Mikäli poliisin yksiköltä pyydetään tietoa salassa pidettävästä, toisen viranomaisen laatimasta tietoaineistosta, on asia siirrettävä ratkaistavaksi tietoaineiston laatineelle viranomaiselle.
(Poliisihallituksen määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2010.)

2.2.7 Poliisihallituksen määräys tietoturvatasoista poliisihallinnossa (2020/2011/81)

Poliisin tietoturvallisuuden jatkuva arviointi ja toiminnan kehittäminen perustuu Valtioneuvoston asetukseen tietoturvallisuudesta valtionhallinnossa (681/2010) määrittämien tietoturvatasojen vaatimuksiin. Poliisihallituksen määräyksen poliisihallinnon tietoturvatasoista (2020/2011/81) mukaan poliisiyksiköiden tulee täyttää tietoturvatasojen perustaso 1.1.2013 mennessä ja 1.1.2015 mennessä kaikkien poliisin yksiköiden tulee täyttää vähintään tietoturvatasojen korotettu taso. Niiden toimintojen osalta missä käsitellään suojaustasojen I ja II tietoja tulee täyttää tietoturvatasojen korkea taso 1.1.2015 mennessä.

Poliisihallinnossa tietoturvatasojen vaatimuksilla käsitetään Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (VAHTI 2/2010) liitteen 5 määrittämien tietoturvallisuustasojen vaatimuksia. Seuraavilla sivuilla on taulukoihin 3-6 koottu Poliisin henkilöstön yleiseen tietoturvallisuusohjeeseen liittyvät keskeisimmät VAHTI 2/2010 liitteen 5 määrittämät tietoturvallisuustasojen yksityiskohtaiset vaatimukset.

	Henkilöstölle asetettavat vaatimukset
Osa-alueen nimi	Osaamisen ja tietoisuuden kehittäminen sekä sanktiot
Tavoitteet	Jatkuvuuden hallinnan ja tiedon turvaamisen osaamiselle on asetettu rooli- tai tehtäväkohtaiset vaatimukset, osaamistaso tunnetaan ja osaamista kehitetään. Organisaatio kannustaa henkilöstöä noudattamaan ja kehittämään hyvää jatkuvuuden hallinnan ja tiedon turvaamisen toimintamallia. Organisaatiossa on sovittu tapa toimia turvallisuuspoikkeamissa ja väärinkäyttötilanteissa.
Suomen erityisvaateet	Työntekijän tekninen valvonta on käsitelty YT-menettelyn mukaisesti. (Laki yksityisyyden suojasta työelämässä, 21§)
Perustason vaatimukset	- Organisaatiossa järjestetään säännöllisesti tietoturvakoulutusta henkilöstölle ja muille avainryhmille. Tietoturvahenkilöstön osaamista kehitetään ja ylläpidetään. - Perehdyttämistilanteessa käsitellään myös tietoturva-asioita. - Muuttuneista tietoturvaohjeista ja –käytännöistä tiedotetaan kaikille organisaatiossa toimiville.
Korotetun tason Vaatimukset	- Organisaatiossa on kirjallinen tietoturvallisuuden koulutusohjelma. - Perehdyttäjällä on kirjallinen lista käsiteltävistä tietoturva-asioista. - Henkilöstön osallistumista koulutuksiin seurataan. - Tietoturvamääräysten ja –ohjeiden rikkomisen seuraukset on kuvattu organisaatiossa ja tiedotettu kaikille organisaatiossa työskenteleville. - Esimies ja alainen käyvät vuosittain keskustelun työn tietoturvavastuista ja osaamisen kehittämisen tarpeista. - Henkilöstön tietoturvaosaamisesta varmistutaan.
Korkean tason lisävaatimukset	- Tietoturvakoulutuksessa otetaan huomioon organisaatiossa ja lähiympäristössä tapahtuneet muutokset ja tietoturvapoikkeamat. - Hyvistä tietoturvateoista annetaan positiivista huomiota.

Taulukko 3: Osaamisen ja tietoisuuden kehittäminen sekä sanktiot (VAHTI 2/2010, liite 5)

	Henkilöstölle asetettavat vaatimukset
Osa-alueen nimi	Henkilöresurssien ja tehtävien hallinta
Tavoitteet	Henkilöstö ja sen käyttö on suunniteltu ja mitoitettu ydintoimintojen jatkuvuuden hallinnan ja tiedon turvaamisen edellyttämällä tavalla. Avainroolit ja –henkilöt on tunnistettu ja varajärjestelyt on suunniteltu.
Perustason vaatimukset	Toteutettavaksi valitut tietoturvatoimenpiteet ja –prosessit on organisoitu ja vastuutettu. Tietoturvallisuuden avainroolit on tunnistettu ja niille on nimetty varahenkilö tai –henkilöt.
Korotetun tason lisävaatimukset	Toteutettavaksi valituista tietoturvaprosesseista tai –toimenpiteistä ja niiden vastuuhenkilöistä on luettelo. Tietoturvallisuuden varahenkilöt on koulutettu tehtäväänsä.
Korkean tason lisävaatimukset	Organisaatiossa on määritelty tehtävät tai roolit, joiden hakijasta tehdään turvallisuusselvitys, ja selvityksen hakuprosessi on dokumentoitu. Organisaatiossa on tehty tietoturvallisuuden osaamiskartoitus.

Taulukko 4: Henkilöresurssien ja tehtävien hallinta (VAHTI 2/2010, liite 5)

	Henkilöstölle asetettavat vaatimukset
Osa-alueen nimi	Erityistilanteissa toimiminen
Tavoitteet	Kriittisten toimintojen häiriöiden hallintaohjeet on laadittu, koulutettu ja toiminta harjoiteltu.
Perustason vaatimukset	Henkilöstö tietää kenelle tietoturvapoikkeamista ja –tapauksista tai niiden uhkista tulee ilmoittaa.
Korotetun tason lisävaatimukset	Tietoturvapoikkeamia selvittävät henkilöt on koulutettu tehtäväänsä.
Korkean tason lisävaatimukset	Organisaatiossa on tietoturvapoikkeamien selvittämiseen koulutettu ryhmä, joka harjoittelee säännöllisesti.

Taulukko 5: Erityistilanteissa toimiminen (VAHTI 2/2010, liite 5)

	Toiminnan prosesseille asetettavat vaatimukset
Osa-alueen nimi	Tietoaineistojen hallinta
Tavoitteet	Asiakirjallisen ja muun tietoaineiston turvallisuudesta huolehditaan sen koko elinkaaren aikana. Organisaatiossa käsitellään tietoaineistoja lakien ja hyvän hallintatavan mukaisesti.
Suomen erityisvaateet	Organisaatiolla on arkistonmuodostussuunnitelma (Arkistolaki 8§), josta käytetään usein myös nimitystä tiedonhallinta- tai tiedonohjaussuunnitelma. Organisaatio pitää luetteloa organisaatioon käsiteltäviksi tulleista ja käsitellyistä asioista (Julkisuuslaki 18§).
Perustason vaatimukset	Työntekijät tietävät miten tietoaineistoja organisaatiossa käsitellään. Organisaation tuottamasta kirjallisesta asiakirjasta käy ilmi kuka sen on laatinut ja milloin sekä sen hyväksymisen tila. Hävitettäväksi tarkoitetut asiakirjat tuhotaan niin, että luottamuksellisuus ja tietosuoja on varmistettu.
Korotetun tason lisävaatimukset	Organisaatiossa on tietoaineistojen käsittelyn kirjallinen ohje, jossa kerrotaan, miten asiakirjat hyväksytään, katselmoidaan ja mikä organisaation aineisto on salassa pidettävää tai muun vaitiolovelvollisuuden alaista.
Korkean tason lisävaatimukset	Organisaatiossa käytössä olevat tietoaineistojen hallinnan välineet tukevat aineistojen luokittelua ja arkistointia.

Taulukko 6: Tietoaineistojen hallinta (VAHTI 2/2010, liite 5)

2.2.8 VAHTI-ohjeisto

Valtiovarainministeriö vastaa valtion tietoturvallisuuden ohjauksesta ja kehittämisestä. Tietoturvallisuuden lähtökohtana on se, että jokainen organisaatio vastaa oman toimintansa tietoturvallisuudesta. Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) tehtävänä on toimia tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen tukena. Johtoryhmän tehtävänä on käsitellä valtionhallinnon tietoturvallisuutta koskevat säädökset, ohjeet, suositukset ja tavoitteet sekä muut tietoturvallisuuden linjaukset sekä ohjata valtionhallinnon tietoturvatoimenpiteitä. Sen tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista sekä edistää

tietoturvallisuuden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta. (Tietoturvallisuus 2012.)

VAHTI kehittää VAHTI-ohjeistusta, joka kattaa kaikki tietoturvallisuuden osa-alueet. Voimassa olevia VAHTI julkaisuja on yhteensä 45 kpl (tilanne 11.3.2012) ja ne ovat luettavissa VM:n Internet sivustolta:
http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/02_tietoturvaohjeet_ja_maaraykset/index.jsp.

2.3 Yhteenveto kehittämistyön viitekehyksistä

Kuten havaitaan, tietoturvallisuuteen liittyy paljon erilaisia viitekehyksiä, jotka ovat osittain päällekkäisiä ja toisiaan sivuavia. Edellä kuvatut viitekehykset liittyvät kaikki valtionhallintoon ja viranomaisiin ja niille ominaista on, että ne ovat kaikki ns. velvoittavia eli viranomaiselle ei jää juuri harkintavaltaa siitä, mitä näistä viitekehyksistä toteutetaan tai otetaan käyttöön. Tietoturvallisuustasojen osalta organisaatio voi halutessaan jättäytyä perustasolle, jättämällä tekemättä luokittelupäätöksen, mutta näin tehdessään se hankaloittaa yhteistyötä sellaisen viranomaisen kanssa, joka käyttää luokitusmenetelmää. Tietoturva-asetus nimittäin velvoittaa viranomaista, luokiteltua asiakirjaa luovuttaessaan, varmistamaan asiakirjan vastaanottajan edellytyksistä käsitellä asiakirjaa asianmukaisesti

3 Tutkimus- ja kehittämismenetelmät

Tieteellisessä tutkimuksessa pyritään luomaan uutta teoriaa ja testaamaan teorioita ja siinä noudatetaan tieteellisen tutkimuksen traditioita. Olennaista siinä ovat tutkimusongelma, tutkimuskysymykset ja niihin vastaaminen yleisesti hyväksyttyjä menetelmiä käyttämällä. Tutkimuksellinen kehittämisessä sen sijaan pyritään ratkaisemaan käytännössä esille tulleita ongelmia tai uudistamaan käytäntöjä ja usein myös luomaan uutta tietoa työelämän käytännöistä. Tutkimuksellinen kehittämistyö voi saada alkunsa erilaisista lähtökohdista, kuten organisaation kehittämistarpeista tai halusta saada aikaan muutoksia. Siihen kuuluu siis käytännön ongelmien ratkaisua ja uusien ideoiden, käytäntöjen, tuotteiden tai palvelujen tuottamista ja toteuttamista. Tieteellisen tutkimuksen ja tutkimuksellisen kehittämistyön ero on pääasiassa toiminnan päämäärissä – halutaanko tuottaa ilmiöistä uutta teoriaa vai saada aikaan myös käytännön parannuksia tai uusia ratkaisuja. (Ojasalo, Moilanen & Ritalahti, 2009, 18-19.)

Tässä kehittämistehtävässä pyritään hyvin konkreettiseen ja käytännönläheiseen ongelmanratkaisuun luomalla uusi malli (yleinen tietoturvallisuusohje) aikaisemman, olemassa olevan tiedon pohjalta.

3.1 Menetelmällinen perusta

Erilaisia tutkimusmetodeja on useita ja tutkimusmetodin valintaan vaikuttaa oleellisesti onko kyseessä perus- vai soveltava tutkimus. Tutkimusmetodi auttaa ja ohjaa tutkijaa hänen suorittaessaan tutkimustaan ja tutkijan tehtävänä on valita oikea tutkimusmetodi vallitsevan tutkimusongelman mukaan. Järvinen & Järvinen (2004, 103) toteavat, että jos tutkimuskysymys sisältää verbejä rakentaa, parantaa, laatia jne., kuuluu tutkimus mitä todennäköisimmin suunnittelutieteen piiriin.

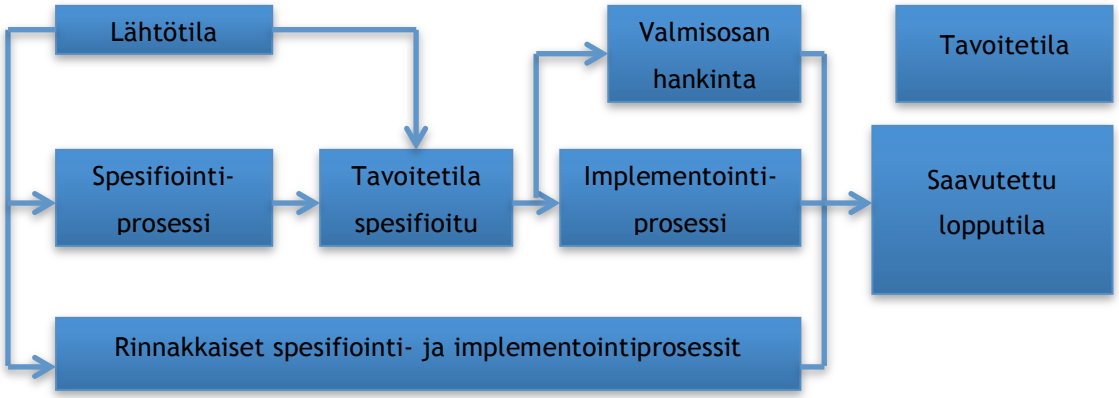
Ojasalo, Moilanen ja Ritalahti (2009, 65) toteavat, että kehittämistehtävään, jolla pyritään konkreettiseen tuotokseen tai esim. suunnitelmaan, mittariin tai malliin, sopii konstruktiivinen tutkimus. Konstruoinnin tuloksena voi syntyä konstrukteja, malleja, metodeja ja toteutuksia eli innovaatioita ja ne voidaan toteuttaa rakentamalla ja arvioimalla (Järvinen & Järvinen 2004, 103). Ojasalo, Moilanan & Ritalahti (2009, 65-68) erottavat konstruktiivisen tutkimuksen omaksi lähestymistavaksi innovaatiosta sen takia, että läheskään kaikki kehittämistyön tuloksena syntyneet tuotokset eivät ole innovaatioita, kuten esim. uusi kirja, yrityksen www-sivusto, palvelujen kehitykseen liittyvä prosessimalli taikka kuten tässä kehittämistyössä henkilöstön tietoturvaohje. Edellä mainitut tuotokset ovat kehitystyön tuloksena syntyneitä rakenteita, joita arvioidaan käytännön hyödyn perusteella ja konstruktiivinen kehittämistyö sopii juuri tämän tyyppisiin kehittämistehtäviin. Konstruktiiviselle tutkimukselle on tyypillistä myös, että käytettävät menetelmät voivat olla kirjavia, sillä lähestymistapa ei sinänsä rajaa pois mitään menetelmää.

Tässä kehittämistehtävässä on tarkoituksena luoda poliisin henkilöstölle tietoturvallisuusohje, jonka avulla voidaan ohjeistuksen lisäksi parantaa henkilöstön tieturvallisuuden tietämystä. Näin ollen kehittämistyö on tarkoituksenmukaista toteuttaa konstruktiivista tutkimusmetodia käyttäen.

Järvisten (2004, 107) mukaan on melkein aina mahdollista tunnistaa konstruoinnin lähtökohta ja myös sen hetkinen ajatus toivotusta lopputilasta. Tavoitetilan kuvaus on siis malli tilanteesta, jossa toivomme asioiden olevan, kun olemme toteuttaneet ideamme. Toteuttaminen käsittää metodin, jonka avulla uskomme saavuttamamme tavoitetilan. Kehittämistyön toteuttamisprosessi voidaan kuvata hyvin yksinkertaisesti seuraavalla kuviolla.

Kuvio 3: Kehittämistyön (innovaation) toteuttamisprosessi (Järvinen & Järvinen 2004, 107)

Järvisten (2004) mukaan lähtötilasta voidaan pyrkiä tavoitetilaan ainakin kolmea polkua pitkin. Jokaiseen polkuun liittyy spesifiointi eli tavoitetilan määrittely. Tavoitetilan määrittelyn jälkeen tapahtuu implementointiprosessi tai valmisosan hankinta. Spesifiointi- ja implementointiprosessi voivat olla myös samanaikaisia. Implementointiprosessissa kysytään: Miten voimme saada aikaan halutun tilanmuutoksen? Valmisosan hankinnalla tarkoitetaan konkreettisen tuotteen hankkimista valmisosana, jotta pyörää ei tarvitsisi keksiä uudelleen.



Kuvio 4: Vaihtoehtoisia tapoja toteuttaa innovaatio (Järvinen & Järvinen 2004, 108)

Tavoitetila heijastaa innovaation suunnittelijoiden ja päättäjien arvoja ja se esittää, miten asioiden pitäisi olla. Aina ei kuitenkaan saavuteta tavoitetilaa, vaan voidaan jäädä tavoitetilasta taikka mennä tavoitetilan yli eli saavuttaa parempi tulos, kuin osattiin toivoa. (Järvinen & Järvinen 2004, 108.)

Spesifiointiprosessin tarkoituksena on siis tuottaa jonkinlainen kuvaus tavoitetilasta. Jos tutkija pääsee yksin määrittelemään uutta innovaatiota, ei hänen tarvitse sovittaa yhteen useamman intressiryhmän tavoitteita. Implementointiprosessissa tutkimuksen ydinkysymyksenä on, voidaanko tietty innovaatio toteuttaa tai saavuttaa käytettävissä olevilla resursseilla. Spesifiointiprosessin mitä -tavoite tuleekin suhteuttaa implementointiprosessin miten -keinoihin. Implementointiprosessissa voidaan käyttää erilaisia ongelmanratkaisun heuristiikkoja, kuten esimerkiksi ongelmanreduktion heuristiikkaa, jossa pääongelma pyritään ratkaisemaan ratkaisemalla pienempiä osa-ongelmia kerrallaan. Tila-siirtymä-heuristiikan avulla ongelma pyritään ratkaisemaan etenemällä lähtötilasta kohti tavoitetilaa peräkkäisten tilanmuutosten kautta. (Järvinen & Järvinen 2004, 109-110.)

Rinnakkaisia spesifiointi- ja implementointiprosesseja käytetään yleensä innovaation asteittaisessa kehittämisessä, sillä usein on vaikea kuvitella sellaista, mitä ei ole vielä olemassa. Tällöin tavoitetilan määrittely on hankalaa ja sen sijaan päädytään kokeilemaan tavoitetilan

hahmotuksia ja saman aikaisesti toteuttamaan niitä esimerkiksi prototyyppejä kehittämällä. Asteittain kehittämisen pulmana on, milloin on syytä lopettaa kehittäminen? (Järvinen & Järvinen 2004, 111-112.)

Suunnittelutieteen rakentamisen tuloksia ovat käsitteistö, malli, metodi ja realisointi. Käsitteistö voidaan luoda jollekin uudelle aihealueelle. Koko käsitteistöä ei yleensä uusita, jotta uuden innovaation käyttö onnistuisi paremmin käyttäen entuudestaan tunnettuja käsitteitä. Innovaation uusi malli kuvaa tavallisesti mahdollista innovaation realisaatiota ja se sisältää jonkin hyötynäkökohdan innovaatiosta. Mitä yksityiskohtaisempi tavoitetilan kuvaus on, sitä paremmin pystytään arvioimaan sen toteuttamiskelpoisuus, saavutettavat hyödyt sekä muut vaikutukset. Konstruktiivisen tutkimuksen ainoana loppusuoritteena voi syntyä metodi, jonka mukaan uusi innovaatio voidaan toteuttaa eli metodia noudattamalla pitäisi pystyä siirtymään lähtötilasta tavoitetilaan tai ainakin lähelle sitä. (Järvinen & Järvinen 2004, 113-114.)

Järviset (2004, 118-124) suosittavat innovaation arvioinnissa mm. seuraavia kriteereitä: helppokäyttöisyyttä, hyödynnettävyyttä, mallin totuudenmukaista kuvausta realisaatiosta sekä johdonmukaisuutta. He muistuttavat myös, että tärkeää on aina arvioida myös, missä määrin asetetut tavoitteet saavutettiin. Ojasalo, Moilanen & Ritalahti (2009, 68) toteavat, että kehitetyn ratkaisun toimivuutta arvioidaan käytännössä eli markkinoilla tai organisaation sisällä. Käytössä on kolme eritasoista testiä. Ratkaisu läpäisee heikon markkinatestin, jos se toimii kohdeorganisaatiossa käytännössä. Keskivahvan markkinatestin läpäisemiseksi on usean organisaation otettava ratkaisu käyttöön ja vahvan markkinatestin läpäisy vaatii, että ratkaisun käyttöön ottaneet organisaatiot menestyvät paremmin kuin ne, jotka eivät ole ottaneet sitä käyttöön.

3.2 Lähtötila

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (Tietoturva-asetus) astui voimaan 1.10.2010 ja sen mukaan jokaisen valtionhallinnon organisaation tulee toteuttaa tietoturvallisuuden perustaso kolmen vuoden päästä ja korkeampi tietoturvallisuuden taso viiden vuoden päästä asetuksen voimaantulosta. Poliisihallituksen antaman määräyksen mukaan poliisiyksiköiden tulee täyttää perustaso 1.1.2013 mennessä ja 1.1.2015 mennessä tulee jokaisen poliisin yksikön täyttää vähintään tietoturvatasojen korotettu taso. VAHTI 2/2010 liitteessä 5 on määritelty eri tietoturvatasojen mukaisia poliisin henkilöstölle asetettuja vaatimuksia. Tietoturvatasovaatimusten mukaan henkilöstölle on järjestettävä tietoturvakoulutusta ja henkilöstön tietoturvaosaamista ja tietoutta on lisättävä.

Sisäasiainministeriön hallinnonalan määräysten ja poliisihallinnon tietoturvaperiaatteiden mukaisesti poliisihallinnon henkilöstölle tulee järjestää vähintään joka toinen vuosi tietoturva-

koulutusta. Sisäasiainhallinnon tietoturvallisuuden verkkokoulutuksen osa I sisältää tietoturvallisuuden perusasioita ja osa II salassa pidettävien tietoaineistojen käsittelyä.

Jokaisen poliisin henkilökuntaan kuuluvan tulee suorittaa verkkokoulutuksen osa II mahdollisimman pian ja viimeistään 31.12.2011. Koulutuksen osa I tulee olla suoritettuna ennen osaan II siirtymistä. Poliisiorganisaation palvelukseen tulevien on suoritettava tietoturvallisuuden verkkokoulutuksen osat I ja II kahden kuukauden kuluessa palvelussuhteen alkamispäivämäärästä lukien.

Saavuttaakseen vaaditun tietoturvallisuuden tason on teknisten ratkaisujen kehittämisen ja asiantuntijoiden osaamisen lisäämisen lisäksi parannettava henkilöstön tietoturvaosaamista ja -tietoutta. Hyvän tietoturvallisuuden toteuttamisesta suuri osa on ohjeita ja toimintatapoja - ihmisten rooli on keskeinen, eikä pelkästään teknologian avulla voida saavuttaa riittävää tietoturvallisuuden tasoa. Poliisiyksiköillä on olemassa omia tietoturvallisuusohjeita, mutta tähän saakka on poliisihallinnolta puuttunut yhteinen henkilöstön tietoturvallisuusohje, johon on koottu keskeisimmät tietoturvallisuusohjeet henkilöstön näkökulmasta tarkasteltuna.

3.3 Tavoitetila

Poliisihallituksen tietoturvapäällikkö Samuli Bergströmin asetti tämän kehittämistehtävän tavoitteeksi laatia poliisiorganisaatiolle poliisin henkilöstön yleinen tietoturvallisuusohje. Ohjeen tulisi koota yhteen hajallaan olevat tietoturvallisuuteen liittyvät määräykset ja ohjeet yhdeksi selkeäksi kokonaisuudeksi henkilöstön käyttöön.

Tietoturvallisuusohjeen tehtävänä on kertoa lyhyesti ja selkeästi tietoturvallisuuteen liittyvistä määräyksistä, ohjeista ja toimenpiteistä sekä opastaa käytännönläheisesti poliisin henkilöstöä toteuttamaan tietoturvallista työskentelyä kaikessa työssään. Tavoitteena on myös, että tietoturvallisuusohjeen avulla lisätään henkilöstön tietoturvaosaamista ja tietoturvatietoutta sekä motivoidaan näin ihmisiä toimimaan tietoturvallisesti jokapäiväisessä toiminnassaan. Lisäksi tietoturvallisuusohje voi toimia myös tietoturvakoulutuksen suunnittelun apuna.

Tavoitetilan mukaisiksi kriteereiksi kehittämistyössä muodostuivat seuraavanlaiset kriteerit:

- Ohjeesta tehdään poliisihallinnon yleinen tietoturvaohje, joka on tarkoitettu henkilöstön eli ns. loppukäyttäjien perus tietoturvaohjeeksi.
- Ohjeessa kuvataan tietoturvallisuuden perusvaatimukset ja ohjataan tarvittaessa hakemaan lisätietoa muusta ohjeistuksesta.
- Ohjeen on oltava kompakti ja helppolukuinen.
- Ohje ei ole ristiriidassa olemassa olevien ohjeiden kanssa.
- Ohjetta tulee voida käyttää valtakunnallisesti riippumatta laitoksesta tai yksiköstä.

- Ohje sopii niin kenttä- kuin toimistohenkilöstöllekin.
- Ohje vastaa tietoturvatasojen peruskäyttäjän tietoturvaohjeen vaatimukseen (VAHTI 2/2010, liite 5.1)

3.4 Toteutus

Kehittämistyö toteutettiin keräämällä yhteen poliisin henkilöstön eli loppukäyttäjien kannalta tärkeimmät poliisin tietoturvallisuuteen kuuluvat viitekehykset, jotka koostuivat pääosin lainsäädännöstä, Poliisihallituksen ja SM:n poliisiosaston määräyksistä ja ohjeista sekä Valtiovarainministeriön VAHTI -ohjeista.

Poliisin henkilöstön yleistä tietoturvallisuusohjetta varten käytiin läpi edellä mainitun materiaalin lisäksi myös Poliisin Intranet -sivuston kautta löydettyjä erillisiä ja hajanaisia tietoturvallisuusohjeita. Tästä materiaalista valittiin poliisin henkilöstön eli ns. loppukäyttäjän kannalta oleelliset tietoturvallisuuteen liittyvät määräykset, ohjeet ja neuvot, jotka kerättiin yhteen tähän kehittämistyöhön.

Laadittu Poliisin henkilöstön yleisen tietoturvallisuusohjeen luonnos annettiin luettavaksi Poliisihallituksen tietoturvapäällikölle sekä poliisin tietoturvatyöryhmän jäsenille. Poliisin tietoturvatyöryhmä koostuu eri poliisin yksiköiden tietoturvapäälliköistä ja -vastaavista. Heidän antamansa palautteen perusteella tietoturvallisuusohjeeseen tehtiin vielä muutoksia. Varsinaisen tietoturvallisuusohjeen lisäksi laadittiin erillinen Tietoturvallisuuden huoneentaulu, johon on koottu tietoturvallisuuden keskeisimmät ohjeet joiden tarkoituksena on toimia muistilistana sekä siihen on varattu tila oman yksikön tietoturvavastaavien yhteystiedoille ja muistiinpanoille. Huoneentaulun voi tulostaa ja laittaa paikkaan jossa se on helposti luettavissa.

3.5 Saavutettu lopputila

Kehittämistyönä laadittu Yleinen tietoturvaohje poliisin henkilöstölle luovutettiin Poliisihallituksen tietoturvapäällikölle ja se on tarkoitus julkaista Poliisin Intranetissä sekä ottaa samassa yhteydessä virallisesti käyttöön poliisihallinnossa. Koska ohjetta ei ole vielä tämän raportin laatimisen aikana julkaistu eikä otettu käyttöön, ei siitä ole myöskään vielä saatu kokemuksia, joilla saavutettua lopputilaa voisi arvioida.

Tämän kehittämistyön tuloksena on syntynyt yksi yhteinen, poliisin henkilöstölle tarkoitettu tietoturvallisuusohje, joka edesauttaa tietoturvallisten työtapojen omaksumista poliisin henkilöstön jokapäiväisessä arjessa sekä luo henkilöstölle yhteiset pelisäännöt tietoturvallisuuden toteuttamisessa poliisihallinnossa ja toivottavasti myös motivoi ihmisiä tietoturvalliseen toimintaan.

4 Kehittämistulokset

Tämä kehittämistyö sai alkunsa siitä, kun oli todettu, että poliisihallinnolta puuttuu yksi koko hallinnon yhteinen, henkilöstölle tarkoitettu tietoturvallisuusohje, johon on koottu tärkeimmät tietoturvallisuuteen liittyvät asiat. Eri poliisin yksiköillä on olemassa omia tietoturvallisuusohjeita, mutta monesti ne ovat vaikeasti löydettävissä, irrallisia sekä usein suunnattu tietoturvallisuuden asiantuntijoille. Ohjeet ovat usein vaikeasti ymmärrettäviä ja teknisiin tietoturvaratkaisuihin pohjautuvia. Jokapäiväiseen työn tekemiseen liittyviä ohjeita on harvassa.

Kehittämistyössä kerättiin yhteen paikkaan poliisin henkilöstölle tärkeimmät tietoturvallisuuteen liittyvät määräykset ja ohjeet yhdeksi kokonaisuudeksi. Tietoturvallisuusohjeen tehtävänä on auttaa hahmottamaan tietoturvallisuuden liittymistä kaikkeen poliisitoimintaan sekä opastaa poliisin henkilöstöä toteuttamaan tietoturvallista työskentelyä mahdollisimman käytännönläheisesti ja samalla kattavasti eri tietoturvallisuuden osa-alueilla. Tietoturvallisuusohjetta voi käyttää käsikirjan tavoin, josta voi tarvittaessa etsiä tietoa käsillä olevasta tietoturvallisuuteen liittyvästä asiasta.

4.1 Tietoturvallisuusohjeen rakenne

Tietoturvallisuusohjeen toisessa luvussa kuvataan lyhyesti tietoturvallisuuden organisointi poliisissa. Kolmas luku sisältää salassa pidettävien tietoaineistojen käsittelyyn liittyvät asiat, kuten esim. suojaustaso, luokitukset sekä tietoaineiston käsittelyvaatimukset eri suojaustasoilla. Neljännessä ja viidennessä luvussa käydään lyhyesti läpi tietoturvallisuuteen liittyviä toimitilojen turvallisuutta sekä tietokoneen käyttöä yleisesti.

Kuudes luku käsittelee Internetiä ja sähköpostia. Luvut 8-14 käsittelevät matkapuhelimen ja Virve-päätelaitteen käyttöä, ajoneuvossa ja yleisellä paikalla työskentelyä, sosiaalista mediaa ja -hakkerointia. Luvussa 14 kuvataan toimintaa ongelmatilanteissa ja luku 15 esittelee tietoturvallisuuden huoneentaulun.

5 Kehittämistyön arviointi

Opinnäytetyön tavoitteena oli tehdä poliisin henkilöstön käyttöön yleinen perustietoturvallisuusohje, jossa hajallaan olevat tietoturvallisuuteen liittyvät määräykset ja ohjeet on koottu yhdeksi kompaktiksi ja helppolukuiseksi kokonaisuudeksi henkilöstön käyttöön. Ohje ei saa olla ristiriidassa olemassa olevien ohjeiden kanssa ja sitä pitää pystyä käyttämään valtakunnallisesti riippumatta poliisilaitoksesta tai yksiköstä. Ohjeen pitää soveltua sekä kenttä- että toimistotehtävissä työskentelevien käyttöön ja sen pitää vastata tietoturvatasojen peruskäyttäjän tietoturvaohjeen vaatimukseen. (VAHTI 2/2010, Liite 5.)

Kehitetyn ratkaisun toimivuutta arvioidaan organisaation sisällä ja sen toimivuutta voidaan arvioida joskus myöhemmin. Tämän takia konstruktiivisen tutkimuksen raporteista voi puuttua lähestymistavalla tyypillinen ratkaisun testaus erityisesti silloin, kun on kyseessä opinnäytetyö tai muu työ, joka on sidottu joltakin osin muun kuin kohdeorganisaation aikatauluihin. (Ojasalo, Moilanen & Ritalahti 2009, 68.)

Tämän kehittämistyön tuotoksena syntyneen yleisen tietoturvallisuusohjeen arviointi toteutettiin aikataulullisista ja resurssisyistä johtuen, antamalla tietoturvallisuusohje luettavaksi poliisin tietoturvatyöryhmän, joka koostuu eri poliisin yksiköiden tietoturvapäälliköistä ja -vastaavista, jäsenille. He arvioivat ohjeen sisältöä ja antoivat siihen omat kommenttinsa sekä muutos- ja korjausehdotuksensa. Saatujen palautteiden perusteella tehtiin ohjeeseen vielä joitain parannuksia ja muutoksia. Tietoturvaohjeen käyttökelpoisuutta ei päästy arvioimaan aikataulullisista syistä. Sen arvioiminen jää myöhempään ajankohtaan, kun tietoturvaohje on saatu henkilöstön käyttöön ja siitä on saatu käyttökokemuksia.

5.1 Hyöty kohdeorganisaatiolle

Poliisin yleinen tietoturvaohje on henkilöstölle eli loppukäyttäjille tarkoitettu tietoturvallisuuden perusteos, josta löytyy tavanomaiset, jokapäiväiseen työhön liittyvät poliisin tietoturvallisuuteen liittyvät vaatimukset, määräykset ja ohjeet. Tietoturvaohjeeseen on sisällytetty tarvittavat viittaukset useisiin lähteisiin, joiden avulla voi tutustua tarkemmin tietoturvallisuuteen liittyviin eri aiheisiin.

Tietoturvaohje on tehty sellaiseen muotoon, että se on valtakunnallisesti käytettävissä riippumatta laitoksesta tai yksiköstä sekä henkilöstön toimenkuvasta ja työtehtävästä. Se on tehty soveltuvaksi niin kenttä-, tutkinta- kuin toimistohenkilökunnallekin. Näin ollen jokainen yksikkö voi käyttää tietoturvaohjetta perusohjeena, johon voidaan tarvittaessa lisätä yksikön omia erityisiä tietoturvaohjeita.

Ohjeen avulla on mahdollista kehittää ja yhdenmukaistaa poliisin tietoturvakäytäntöjä. Sen avulla voidaan lisätä henkilöstön tietoturvatietoutta ja tietoturvataitoja sekä parantaa motivaatiota tietoturvallisempaan työskentelyyn. Tietoturvaohjetta voidaan myös käyttää apuna tietoturvakoulutuksia suunniteltaessa.

Tietoturvallisuusohjeen yksi merkittävimmistä hyödyistä on se, että nyt tietoturvallisuuteen liittyvä ohjeet on nyt koottu yhteen paikkaan, josta se on helposti löydettävissä.

5.2 Hyöty laajemmin

Poliisin henkilöstön yleinen tietoturvallisuusohje on suunnattu poliisin henkilöstölle jokapäiväisen toiminnan tueksi, mutta sitä voidaan käyttää soveltuvin osin myös muissa viranomaisissa, sillä tietoturvallisuusohje pohjautuu pääosin kaikkia viranomaisia velvoittaviin lakeihin ja asetuksiin. Lisäksi tietoturvallisuusohjetta voi hyödyntää soveltuvin osin yksityisellä sektorilla ja jopa ihmisten jokapäiväisessä elämässä ja toiminnassa.

Tietoturvallisuusohjeen pohjalta tai sen avulla on mahdollista suunnitella ja toteuttaa poliisin henkilöstölle suunnattua tietoturvallisuuden kolutusta sekä mahdollisesti kehittää henkilöstön tietoturvallisuustietoisuuteen ja tietoturvallisuusosaamiseen kohdistettuja auditointeja.

5.3 Työn rajoitteet

Tietoturvallisuusohje on laadittu poliisihallintoon ja siksi se ei sellaisenaan sovellu yksityiselle sektorille kaikilta osin. Poliisin tietoturvallisuusvaatimukset perustuvat pitkälti lakeihin ja asetuksiin sekä määräyksiin ja ohjeisiin, joista suuri osa ei koske yksityistä sektoria. Tietoturvallisuusohje on pyritty laatimaan sellaiseen muotoon, että se on sovellettavissa kaikissa poliisin eri yksiköissä, joten siihen ei ole sisällytetty eri yksiköissä mahdollisesti olevia yksityiskohtaisia ohjeita erilaisten tietoturvallisuuteen liittyvien toimenpiteiden toteuttamiseen. Yksikkökohtaiset ja yksityiskohtaiset ohjeet on jokaisen poliisiyksikön itse sisällytettävä tämän ohjeen yhteyteen.

Koska tietoturvallisuusohje on laadittu loppukäyttäjien tarpeisiin, ei siinä ole käsitelty varsinaisia tietoturvallisuuteen liittyviä teknisiä ratkaisuja, eikä se näin ollen sellaisenaan sovellu tietoturvallisuuden teknisten ratkaisujen toteuttamiseen. Toisaalta ohjeesta voi olla apua tietoturvallisuuden teknisiä ratkaisuja suunniteltaessa.

6 Yhteenveto

Tietoturvallisuus on hyvin laaja kokonaisuus, joka liittyy lähes kaikkeen mitä ihminen tekee töissään ja vapaa-aikanaan. Jo pelkästään viranomaisia ja poliisia koskevat lait ja asetukset ovat niin laaja kokonaisuus, että niiden asiasisällön tiivistäminen yhteen kompaktiin ohjeeseen on erittäin haastavaa, ellei jopa mahdotonta. Poliisin henkilöstön yleisessä tietoturvallisuusohjeessa pyrittiin käsittelemään mahdollisimman laajasti, mutta kuitenkin riittävän yleisellä tasolla loppukäyttäjän kannalta keskeisimmät tietoturvallisuuteen ja sen ylläpitämiseen sekä parantamiseen liittyvät asiat.

Poliisin henkilöstön yleisen tietoturvallisuusohjeen laatimisen yhteydessä kerättiin kasaan ja käytiin läpi suuri määrä materiaalia mm. lait, asetukset, määräykset, ohjeet ym., jotka liittyvät tietoturvallisuuteen poliisihallinnossa. Tästä materiaalista poimittiin merkittävimmät poliisin tietoturvallisuuteen liittyvät asiat ja niistä koottiin mahdollisimman kattava, mutta kuitenkin tarpeeksi tiivis ja selkeä paketti poliisin henkilöstön yleiseksi tietoturvallisuusohjeeksi. Ohje annettiin luettavaksi poliisin tietoturvatyöryhmän jäsenille, jotka kommentoivat ohjetta ja joiden kommenttien mukaan ohjeeseen tehtiin tarvittavat muutokset, korjaukset ja lisäykset. Tietoturvallisuusohje laadittiin käsikirjamuotoon, josta voi selailla tarvitsemaansa ohjetta. Tietoturvallisuusohjeissa on myös viittaukset lähdeaineistoon, josta voi tutustua tarkemmin aiheeseen liittyviin lakeihin, asetuksiin, määräyksiin ja ohjeisiin. Ohjeeseen sisällytettiin myös yksinkertaisia ohjeita tietoturvallisuuden toteuttamiseen käytännön työssä. Tietoturvallisuusohjeen yksi merkittävimmistä hyödyistä on se, että nyt tietoturvallisuuteen liittyvä ohjeistus on koottu yhteen paikkaan, josta se on helposti löydettävissä.

Ennen ohjeistuksen julkaisemista, voitaisiin henkilöstölle tehdä kyselytutkimus sen selvittämiseksi millä tasolla henkilöstön tietoturvallisuus on tällä hetkellä. Seuraavan kerran tutkimus voitaisiin tehdä esimerkiksi 6-12 kk:n kuluttua tietoturvallisuusohjeen julkistamisesta ja verrata sen tuloksia ensimmäisen testin tuloksiin. Jälkimmäisessä tutkimuksessa voitaisiin selvittää myös tietoturvallisuusohjeen toimivuus ja käyttökelpoisuus ja näiden tuloksien perusteella ohjetta voitaisiin kehittää edelleen.

Lähteet

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Dosendo.

Heljaste, J-M., Korkiamäki, J., Laukkala, H., Mustonen, J., Peltonen, J. & Vesterinen, P. 2008. Yrityksen turvallisuusopas. Helsinki:Kauppakamari.

Henkilöstön tietoturvaohje. 2006. Vahti 10/2006. Helsinki: Valtiovarainministeriö.

Henkilötietolaki 523/1999. Viitattu 20.10.2011.
http://www.finlex.fi/fi/laki/alkup/1999/19990523

Järvinen, P. & Järvinen, A. 2004. Tutkimustyön metodeista. Tampere: Opinpajan kirja.

Kyrölä, T. 2001. Esimies ja tietoriskin hallinta. Helsinki: WSOY.

Laaksonen, J., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Ohjeistus, t teutus ja lainsäädäntö. Helsinki: Edita.

Laki henkilötietojen käsittelystä poliisitoimessa 761/2003. Viitattu 1.10.2012.
http://www.finlex.fi/fi/laki/alkup/2003/20030761

Laki viranomaisen toiminnan julkisuudesta 621/1999. Viitattu 20.10.2011.
http://www.finlex.fi/fi/laki/alkup/1999/19990621

Leppänen, J. 2006. Yritysturvallisuus käytännössä. Turvallisuusjohtamisen portfolio. Helsinki: Talentum.

Miettinen J. E. 1999. Tietoturvallisuuden johtaminen. Näin suojaat yrityksesi toiminnan. Helsinki: Kauppakaari.

Miettinen, J. E. 2002. Yritysturvallisuuden käsikirja. Helsinki: Kauppakaari.

Määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2020/2010/4030 (1.1.2011 – toistaiseksi). Helsinki: Poliisihallitus.

Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. 2010. Vahti 2/2010. Helsinki: Valtiovarainministeriö.

Poliisihallinnon tietoturvaperiaatteet määräys SMDno/2008/353 (7.8.2008 – 6.8.2013). Helsinki: Sisäasiainministeriö. Poliisiosasto.

Poliisin tietoturvapolitiikka määräys 2020/2010/4157 (1.1.2011 – 1.1.2016). Helsinki: Poliisihallitus.

Puhakainen, P. 2006. A design theory for information security awareness. Luentomoniste. Valtionhallinnon tietoturvallisuuden teemapäivä 15.12.2006. Väitöstutkimus. Oulun yliopisto.

Tietoturvallisuus. Julkisen hallinnon ICT. Valtiovarainministeriö. Viitattu 11.3.2012. http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/02_tietoturvaohjeet_ja_maaraykset/index.jsp

Tietoturvatasot poliisihallinnossa määräys 2020/2011/81 (11.1.2011 – 31.12.2015). Helsinki: Poliisihallitus.

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681. Viitattu 20.10.2011. http://www.finlex.fi/fi/laki/ajantasa/2010/20100681

Yritysturvallisuuden osa-alueet. 2009. Yritysturvallisuuden neuvottelukunta. Viitattu 26.1.2012. http://ek2.ek.fi/ytnk08/fi/yritysturvallisuus.php

Kuviot

Taulukot

Liitteet

Liite 1: Yleinen tietoturvaohje poliisin henkilöstölle

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Yleinen tietoturvaohje poliisin henkilöstölle

Kari Tirronen
Turvallisuusosaamisen koulutusohjelma
Opinnäytetyö
Tammikuu 2013

Sisällys

1 Johdanto

Valtionhallinnon tietoturvallisuuden lähtökohtana on säädöksissä määritellyt tietoturvavelvoitteet, valtioneuvoston periaatepäätös valtion tietoturvallisuuden kehittämisestä ja valtiovarainministeriön VAHTI-tietoturvaohjeet sekä muut linjaukset (Tietoturvallisuus 2012). Poliisin tietoturvaperiaatteet (SM/PO 30.7.2008) noudattavat sisäasiainministeriön asettamia tietoturvallisuuden ja poliisin hallinnonalan tietoturvapolitiikan linjauksia.

Poliisin tietoturvapolitiikan (2020/2010/4157) mukaan poliisi on yksi yhteiskunnan turvallisuusstrategian kriittisiä toimijoita, jonka on pystyttävä säilyttämään toimintakykynsä kaikissa turvallisuustilanteissa. Ydinprosessien toimivuuden sekä toimintakyvyn säilyttämisen kannalta on tietoturvallisuuden ja tietotekniikan kriittisyys tunnistettu poliisihallinnossa ja sen vuoksi tietoturvallisuus toimii kiinteässä yhteistyössä poliisin valmiustoiminnan kanssa.

Poliisin tietoturvallisuuden lähtökohtana on toiminnan jatkuvuuden varmistaminen kaikissa tilanteissa sekä tietojen luotettava, sopimusten ja lainmukainen käsittely riippumatta tiedon olomuodosta. Keskeisenä tavoitteena on poliisin luotettavan maineen turvaaminen kansalaisten sekä yhteistyökumppaneiden näkökulmasta. Tätä luottamusta pidetään yllä tehokkaalla, nykyaikaisella ja tarkoituksenmukaisesti suojatulla tietojenkäsittelyllä. (POHA 2020/2010/4157.)

Tietoturvallisuus kuuluu jokaisen työntekijän vastuulle, eikä vain tietoturvasta vastaaville tahoille. Tämä ohje on laadittu auttamaan poliisihallinnon henkilöstöä (ns. loppukäyttäjiä) tietoturvallisuuden toteuttamisessa jokapäiväisessä työssään. Ohjeeseen on koottu olemassa olevista ohjeista loppukäyttäjän kannalta tärkeimmät tietoturvallisuusohjeet. Jokaisen työntekijän tulisi tutustua näihin tietoturvallisuudesta annettuihin ohjeisiin sekä tarvittaessa myös tietoturvallisuutta ohjaaviin tarkempiin määräyksiin ja ohjeisiin sekä lainsäädäntöön.

2 Tietoturvallisuuden organisointi poliisissa

Poliisin tietoturvapolitiikan (2020/2010/4157) mukaan poliisin tietoturvallisuutta johtaa poliisiylijohtaja. Poliisihallitukseen sijoitettu poliisin tietoturvapäällikkö vastaa poliisihallinnon tietoturvallisuustoiminnan ja tietosuojan ohjaamisesta, valvonnasta, kehittämisestä ja yhteensovittamisesta sekä poliisin ylimmän johdon raportoinnista. Erikseen asetettava poliisihallinnon tietoturvatyöryhmä tukee poliisin tietoturvatoiminnan kehittämistä sekä seuraa poliisin tietoturvatoimintaa.

Jokaisen poliisin yksikön johto vastaa yksikön tietoturvallisuudesta, tietoturvatietoudesta ja asenteiden kehittämisestä. Poliisin yksiköissä on nimetty tietoturvapäällikkö tai tietoturvavastaava. Jos yksikössä ei ole nimettyä tietoturvapäällikköä tai -vastaavaa, tehtäviä hoitaa yksikön turvallisuuspäällikkö. Jokaisen työntekijän velvollisuus on selvittää itselleen kuka on oman yksikön tietoturvapäällikkö tai -vastaava. (POHA 2020/2010/4157.)

Poliisihallinnon jokaisen yksikön, sen palveluksessa olevan henkilön sekä jokaisen poliisin tietoja käsittelevän tulee noudattaa annettuja määräyksiä, ohjeita sekä turvallisia toiminta- ja työskentelytapoja. Jokaisen tehtävänä on tunnistaa ja ehkäistä tietoturvariskejä sekä raportoida havaitsemistaan mahdollisista tietoturvallisuuden puutteista. Lisäksi jokaisen tehtävänä on tehdä aloitteita tietoturvallisuuden kehittämiseksi. Esimiesten tehtävänä on alaisten tukeminen ja ohjaaminen sekä sen varmistamien, että heidän vastuualueeseensa sisältyvät tietoturvamenettelyt suoritetaan asianmukaisesti. Esimiehellä on myös vastuu käyttöoikeuksista ja niiden poistamisesta. (POHA 2020/2010/4157.)

3 Poliisin salassa pidettävien tietoaineistojen käsittely

Määräys poliisin salassa pidettävien tietoaineistojen käsittelystä (2020/2010/4030) astui voimaan 1.1.2011 ja se sisältää salassa pidettävien tietoaineistojen käsittelyssä noudatettavat periaatteet poliisihallinnossa. Määräys perustuu lakiin viranomaisen toiminnan julkisuudesta (621/1999) sekä 1.10.2010 voimaan tulleeseen Valtioneuvoston asetukseen tietoturvallisuudesta valtionhallinnossa (681/2010). Määräys kumoaa Sisäasianministeriön määräyksen Poliisihallinnon tietoturvaperiaatteet (SMDno/2008/353) kappaleiden Tietoturvallisuus, Tietoaineiston määritelmä sekä yhdistelmä salassa pidettävän tietoaineiston käsittelystä poliisissa osalta (sivut 19-23).

Määräyksen laatimisessa on otettu huomioon sisäasianhallinnon voimassa oleva ohjeistus sekä Valtiovarainministeriön ohje tietoturvallisuudesta annetun asetuksen täytäntöönpanosta (VAHTI 2/2010), jota ohjetta voidaan käyttää tarkentavana asiakirjana mikäli tässä määräyk-

sessä tai tarkentavassa poliisihallinnon ohjeissa ei asiaa ole ohjeistettu (POHA 2020/2010/4030).

Salassa pidettävän aineiston käsittelyssä on noudatettava erityistä huolellisuutta. Virkamiehen ja julkisyhteisön työntekijän salassapitovelvollisuuden rikkomisesta ja muiden henkilöiden salassapitorikoksesta ja rikkomuksesta säädetään rikoslaissa. (POHA 2020/2010/4030.)

Lähtökohtaisesti viranomaisen asiakirjat ovat julkisia, ellei niitä ole laissa määritelty salassa pidettäviksi. Jokaisella on oikeus saada tieto viranomaisen asiakirjasta, joka on julkinen. Jokaisella on myös oikeus saada tieto hänestä itsestään viranomaisen asiakirjaan sisältyvistä tiedoista, jollei laissa toisin säädetä.

Laki viranomaisen toiminnan julkisuudesta (1999/621) 24 §:ssä on luettelo viranomaisen salassa pidettävistä asiakirjoista. Julkisuuslain 24 §:n 32 kohtaa sisältävä luettelo on hallituksen esityksen mukaan tarkoitettu tyhjentäväksi.

Asiakirjan käsite on julkisuuslaissa laaja. Asiakirjoja ovat mm. kirjallinen ja kuvallinen esitys, ATK-tallenne, muu tekninen tallenne, kartta ja taulukko, videot ja nauhat.

Julkisuuslaki 5 §:n mukaan viranomaisen asiakirjoja ovat viranomaisen hallussa olevat, jonkin asian käsittelyä varten:

- laatimat,
- hankkimat,
- teettämät ja
- takavarikoimat asiakirjat

Julkisuuslaki 5 §:n mukaan viranomaisen asiakirjoja eivät sen sijaan ole:

- virkamiehelle tai luottamushenkilölle hänen muun tehtävänsä tai asemansa vuoksi lähetetty asiakirja.
- virkamiehen tai viranomaisen toimeksiannosta laatima muistiinpano tai luonnos, jos niitä ei ole annettu esittelyä tai muuta asian käsittelyä varten.
- viranomaisen sisäistä käyttöä, kuten esim. koulutusta ja tiedonhakua varten hankitut asiakirjat.
- asiakirja, joka on laadittu tai annettu viranomaiselle yksityisen lukuun suoritettavaa tehtävää varten.
- löytötavarana jäänyt tai toimitettu asiakirja.

Salassapidon arviointi tulee tehdä jo asiakirjaa laadittaessa. Luokitusmerkinnän tekemisestä asiakirjaan päättää asiakirjan allekirjoittaja (esim. tutkinnanjohtaja) tai työjärjestyksessä

erikseen määrätty henkilö. Jos asiakirjaa joudutaan myöhemmin muokkaamaan, tekee salassapidon arvioinnin asiakirjan muokkaaja tai mahdollinen allekirjoittaja. (POHA 2020/2010/4030.) Aineistojen luokitteluun liittyvät tilanteet esim. asiakirjojen sisällön ja turvattavien etujen suhteen ovat niin moninaisia, että yksityiskohtaisen ja tyhjentävän ohjeistuksen antaminen ei ole mahdollista.

Salassapitomerkintä on tehtävä viranomaisen asiakirjaan, joka annetaan asianosaiselle ja joka on salassa pidettävä toisen tai yleisen edun vuoksi. Merkintä on suositeltavaa tehdä myös salassa pidettävään asiakirjaan, joka annetaan toiselle viranomaiselle tai sille, joka viranomaisen toimeksiannon perusteella käsittelee salassa pidettäviä tietoja. Salassapitomerkintä tehdään pääsääntöisesti asiakirjan ensimmäiselle sivulle oikeaan yläkulmaan. Merkinnästä tulee käydä ilmi, miltä osin asiakirja on salassa pidettävä ja mihin salassapito perustuu sekä mille suojaustasolle tietoaineisto luokitellaan. Laajassa asiakirjassa, joka sisältää eritasoisia ja eri perustein salassa pidettävää aineistoa, on esim. kevyemmin tai eri perusteella salassa pidettävät aineistot hyvä leimata erikseen ja niistä tehtävä merkintä ensimmäiselle sivulle. Jos kyseessä on suojaustaso I tai II laitetaan leima jokaiselle sivulle ja sivuun punainen poikkiviiva. (POHA 2010/2010/4030.)

Luokitusmerkintä voidaan jättää tekemättä, jos kaikki asiakirjaa käsittelevät ovat tietoisia asiakirjan salassapidosta ja menettelytavoista taikka kun salassapitovelvollisuus ja siitä johtuvat käsittelyvaatimukset ovat voimassa vain lyhyen ajan tai silloin, kun asiakirjassa on vain joitakin salassapitovelvollisuuden piiriin kuuluvia tietoja ja kaikki asiakirjaa käsittelevät ovat tietoisia sen luonteesta (POHA 2020/2010/4030).

Tietoa salassa pidettävän asiakirjan sisällöstä saa antaa vain viranomainen tai se virkamies, jolle tällainen oikeus on nimenomaisesti annettu. Tietoturvallisuuden varmistamiseksi on jokaisen asiakirjan julkisuus selvitettävä tapauskohtaisesti silloin, kun joku pyytää asiakirjaa nähtäväkseen tai saadakseen siitä kopion. Tämä on hyvä muistaa varsinkin rikosilmoitusjäljennöksiä ja esitutkintapöytäkirjoja luovutettaessa. Salassapitoa ei saa ulottaa laajemmalle kuin suojattava etu vaatii. Jos asiakirjasta vain osa on salassa pidettävää, on viranomaisen annettava asiakirjasta tieto muilta osin. Kieltäytyessään antamasta tietoa asiakirjasta, on viranomaisen tehtävä päätös asetetussa määräajassa sekä perusteltava päätöksensä. (POHA 2020/2010/4030.)

3.1 Suojaustasot

Määräyksen (POHA 2020/2010/4030) mukaan salassa pidettävien tietoaineistojen suojaustasot ovat seuraavat:

I Suojaustaso (ST I)

Asiakirja sisältää äärimmäisen arkaluonteista, salassa pidettävää tietoa, jonka paljastuminen tai käyttö aiheuttaisi erityisen suurta vahinkoa yleisille eduille.
Esim. poikkeusoloihin liittyviä suunnitelmia ja selvityksiä ym.

II Suojaustaso (ST II)

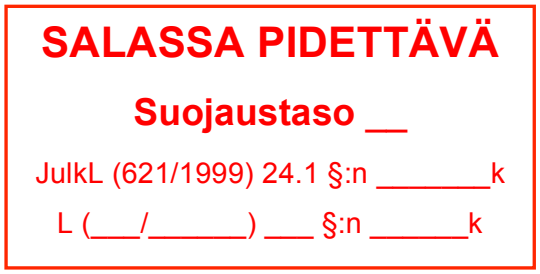
Asiakirja sisältää erittäin arkaluonteista, salassa pidettävää tietoa, jonka paljastuminen tai käyttö aiheuttaisi merkittävää vahinkoa yleisille eduille.
Esim. osa valmiussuunnitelmista, tiedustelutiedoista ym.

III Suojaustaso (ST III)

Asiakirja sisältää salassa pidettävää tietoa, jonka paljastuminen tai käyttö aiheuttaisi vahinkoa yleisille tai yksityisille eduille ja oikeuksille.
Esim. arkaluontoiset henkilötiedot, poliisin erityisryhmien taktiset ohjeet jne.

IV Suojaustaso (ST IV)

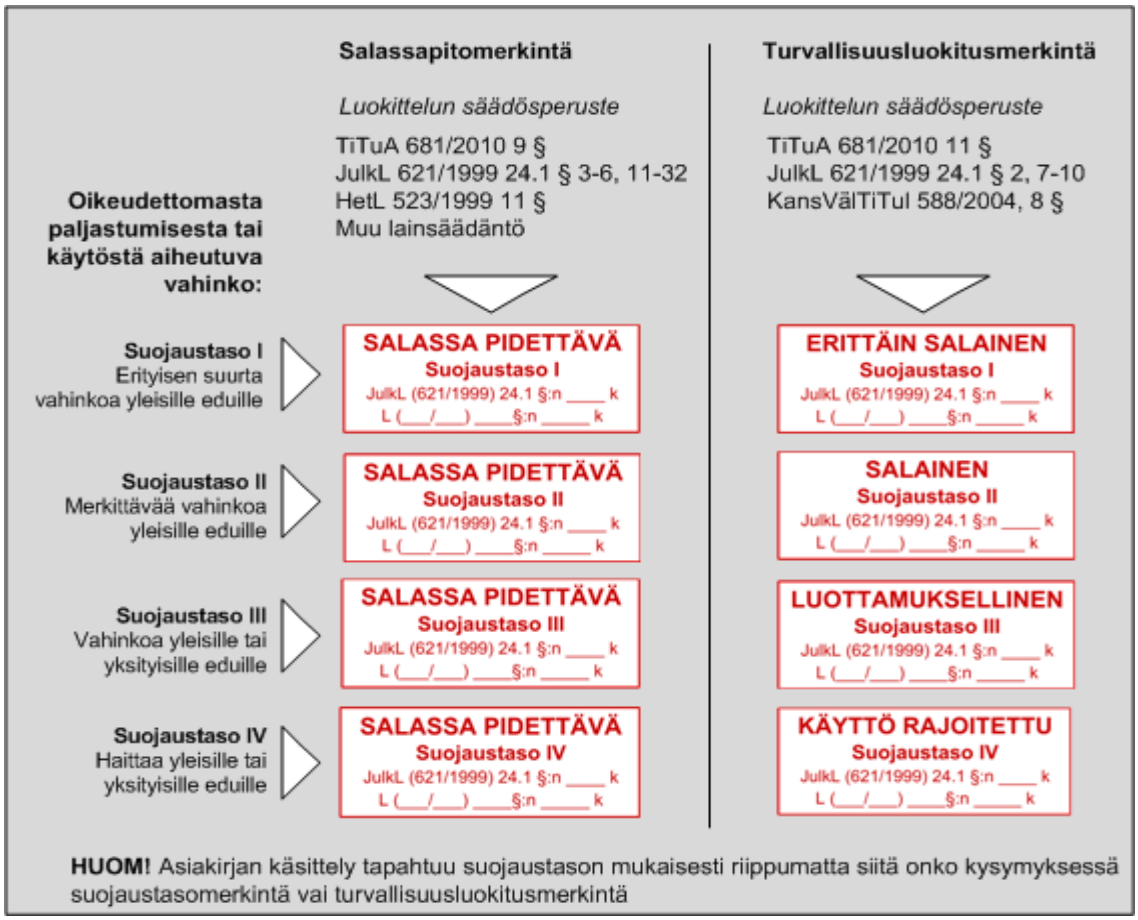
Asiakirja sisältää salassa pidettävää tietoa, jonka paljastuminen tai käyttö aiheuttaisi haittaa yleisille tai yksityisille eduille tai heikentäisi viranomaisen toimintaedellytyksiä. Tähän luokkaan luokiteltavalle aineistolle on tyypillistä laaja käsittelytarve, korkea käytettävyys, soveltuvuus päivittäiseen työskentelyyn ja tiedon paljastumisen aiheuttama vähäinen vahinko salassa pidon perusteena olevalle asialle.
Esim. koko hallinnon laajuiset salassa pidettävät ohjeet, muut kuin arkaluonteiset henkilötiedot jne.



Kuva 1: Suojaustasoa osoittava leima

SALASSA PIDETTÄVÄ (suojaustasot I – IV) -leimaan kirjoitetaan suojaustasoa osoittava numero. Sitä käytetään asiakirjoissa, jotka sisältävät joko julkisuuslain 24 § 1 momentin 1, 3-6 sekä 11 -32 kohtien tai muussa laissa määriteltyä salassa pidettävää tietoa.

Tämän lisäksi leimaa voidaan käyttää suojaustasolla IV asiakirjoihin, joiden luovuttaminen on viranomaisen harkinnassa tai joita saadaan lain mukaan luovuttaa vain määrättyyn tarkoitukseen (esim. henkilörekisterit) ja tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa haittaa yleiselle tai yksityiselle edulle tai heikentää viranomaisen toimintaedellytyksiä.



Kuva 2: Tietoaineistojen suojaustasot ja luokitusmerkinnät (POHA 2020/2010/4030)

Turvallisuusluokitusmerkintää (TL) saa käyttää vain niissä tapauksissa, joissa salassa pidettävän tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa eritasoista vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muille julkisuuslain 24 § 1 momentin 2,7 - 10 kohdassa tarkoitetuille yleisille eduille. Esimerkiksi suojelupoliisin ja muiden viranomaisten asiakirjat, jotka koskevat valtion turvallisuuden ylläpitämistä ja jotkin tieto- ja viestijärjestelmiä koskevat asiakirjat. Turvallisuusluokiteltua aineistoa käsitellään suojaustasoluokille annettujen vaatimusten mukaisesti. (POHA 2020/2010/4030.)

3.2 Henkilötietojen luokitus ja merkinnät

Henkilötietojen käsittelyä ja henkilörekistereitä ohjaavat julkisuuslaki, henkilötietolaki, laki henkilötietojen käsittelystä poliisitoimessa (761/2003) sekä useat eri henkilötietojen käsittelyä koskevat erityislait. Poliisin henkilörekistereiden ja niihin sisältyvien tietojen julkisuus- ja salassapitoperusteet sekä luokitusta koskevat vaatimukset ovat samoja kuin muissakin asiakirjoissa. (POHA 2020/2010/4030.)

Arkaluonteisia henkilötietoja (henkilötietolaki 523/1999; 11 §) sisältävät asiakirjat luokitellaan pääsääntöisesti suojaustasolle III. Arkaluonteinen henkilötieto kuvaa tai on tarkoitettu kuvaamaan:

- rotua tai etnistä alkuperää
- henkilön yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista
- rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta
- henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia
- henkilön seksuaalista suuntautumista tai käyttäytymistä, taikka
- henkilön sosiaalihuollon tarvetta tai hänen saamiaan sosiaalihuollon palveluja, tukitoimia ja muita sosiaalihuollon etuuksia.

Muita kuin arkaluonteisia henkilötietoja sisältävät asiakirjat luokitellaan suojaustasolle IV, mikäli se on suojattavan edun vuoksi tarpeen. (POHA 2020/2010/4030.)

Henkilötietoja Henkilötietolaki 3.1 §:n 1 kohdan mukaan ovat kaikenlaiset:

- luonnollisia henkilöitä taikka
- hänen ominaisuuksiaan kuvaavat merkinnät

jotka voidaan tunnistaa

- häntä tai
- hänen perhettään tai
- hänen kanssaan yhteisessä taloudessa eläviä koskeviksi

Myös henkilötietoja sisältäviä luokittelemattomia asiakirjoja käsitellään lähtökohtaisesti suojaustason IV mukaisesti. Henkilötunnuksen sisältäviä asiakirjoja on käsiteltävä suojaustason IV mukaisesti, ellei asiakirjan sisällön perusteella asiakirjaa kuulu käsitellä korkeamman suojaustason vaatimuksen mukaisesti. (POHA 2020/2010/4030.) Julkisuuslaki 24 § sisältää yksityiskohtaiset määräykset erilaisten henkilötietojen salassapidosta.

3.3 Tietoaineistojen käsittelyvaatimukset

3.3.1 Tietoaineiston hallussapito- ja käsittelyoikeudet

I ja II suojaustason tietoaineistoa saavat käsitellä vain vastaanottajaksi merkityt henkilöt. Käyttöoikeus voidaan antaa ainoastaan henkilöille, joilla työtehtävänsä vuoksi on tarve saada tietoja kyseisestä tietoaineistosta. Hallussapito- ja käsittelyoikeudet ovat rajattu hyvin pienelle joukolle työntekijöitä. Poliisiyksikössä pidetään luetteloa niistä työtehtävistä, joissa on oikeus käsitellä suojaustason I tai II edellyttäviä asiakirjoja. (POHA 2020/2010/4030.)

Varmista tietoturvapäälliköltä tai -vastaavalta aina ennen I ja II suojaustason tietoaineiston vastaanottamista, että olet oikeutettu ottamaan vastaan ja käsittelemään asiakirjaa.

III ja IV suojaustason tietoaineistoa saavat käsitellä kaikki poliisihallinnon virkamiehet ja työntekijät. Tämä oikeus on kuitenkin vain sellaiseen materiaaliin, joka liittyy omaan työtehtävään (POHA 2020/2010/4030).

3.3.2 Tietoaineiston käsittely, tallennus, kopiointi ja tulostus

Suojaustasoihin I ja II kuuluvien asiakirjojen käsittelyn on oltava reaaliaikaisesti jäljitettävissä koko asiakirjan elinkaaren ajan eli kukin asiakirja on kirjattava ja luovutettava allekirjoitusta vastaan ja niistä on pidettävä käsittelylokia.

Suojaustason I tietoaineistoa varten on yksikössä oltava erilliset vain tätä tarkoitusta varten olevat, tietoverkosta erillään olevat laitteet. Suojaustason II - IV tietoaineistoa saa käyttää hallinnonalan tietokoneilla (POHA 2020/2010/4030).

Suojaustasolle I ja II luokiteltuja salassa pidettäviä tietoaineistoja saa käsitellä vain tiloissa, joissa pääsy on rajattu tunnistetuille henkilöille kuten esim. tilat joihin vain poliisilla on pääsy. Tulostaminen on sallittu ainoastaan laitekohtaisella oheistulostimella ja kaikki tulosteet on numeroitava sekä niistä on pidettävä kirjaa. Tietoaineiston tallentaminen tietovälineelle on sallittu vain kun kyseinen tieto on vahvasti salattu. (POHA 2020/2010/4030.) Tiedostojen salausta käsitellään kappaleessa ”Sähköpostin ja tiedostojen salaaminen”.

Suojaustason III - IV tietoaineistoa saa tulostaa verkkotulostimella, jos tulostettu asiakirja noudetaan välittömästi tulostimelta. Tulostettaessa on aina varmistettava, mille verkkotulostimelle tulostus tapahtuu (POHA 2020/2010/4030).

Suojaustason III - IV tietoaineiston tallentamisessa on huolehdittava, että tietoa voivat käsitellä vain siihen oikeutetut henkilöt. Jos tallennus (ST III - IV) tapahtuu siirrettävälle tietovälineelle, on tietoaineisto vahvasti salattava (POHA 2020/2010/4030).

3.3.3 Tietoaineiston säilytys

I ja II suojaustason asiakirjat tulee kirjata omiin, erittäin salaisten (ST I) ja salaisten (ST II) asiakirjojen diaariin, joille molemmille on määrätty oma vastuullinen hoitajansa.

Paperimuotoiset (ST I - II) asiakirjat ja niiden luonnokset on säilytettävä ja arkistoitava holvissa tai murtosuojatussa kaapissa tai vastaavassa.

III-IV suojaustason paperiset asiakirjat on säilytettävä lukitussa kaapissa tai vastaavassa eli jokaisen tulee huolehtia siitä, että em. aineistoa ei jää lojumaan työpöydille, verkkotulostimille ym.

III - IV suojaustason asiakirjat kirjataan julkisten asiakirjojen diaariin. Diaaritiedot ja otsikot eivät saa sisältää suojattavaa tietoa.

(POHA 2020/2010/4030)

3.3.4 Tietoaineiston kuljettaminen ja käsittely virkapaikan ulkopuolella

I suojaustason tietoaineiston vieminen virkapaikan ulkopuolelle ilman yksikön päällikön lupaa on kielletty.

II suojaustason tietoaineistoa saa kuljettaa virkapaikan ulkopuolelle välttämättömiin työtehtäviin liittyen vain niiden käsittelyyn oikeutettu henkilö ja vain yksikön päällikön erillisellä päätöksellä.

Yksikön päällikön päätökset on kirjattava tietoturvapäällikön ylläpitämään kirjaan.

III ja IV suojaustason tietoaineistoa saa jokainen kuljettaa virkapaikan ulkopuolelle, mutta kuitenkin vain työtehtäviin liittyen.

Jos virkapaikalta ulos kuljetettava III - IV suojaustason tietoaineisto on tallennettu tietovälineelle, on se vahvasti salattava ja aineistoa on käsiteltävä siten, että kukaan ei vahingossakaan voi saada käsiinsä suojattavaa tietoa.
(POHA 2020/2010/4030)

3.3.5 Tietoaineiston toimittaminen vastaanottajalle

Suojaustason I tietoaineistoa voidaan lähettää vain kuriirin välityksellä eikä koskaan sähköisessä tietoverkossa sillä asiointikortin varmenne ja verkon turvataso eivät ole riittävän vahvoja tähän luokkaan kuuluvien tietoaineistojen käsittelyyn. Aineisto on pakattava sinetöityyn mustaan kirjekuoreen tai tietoaineistopussiin ja sen jälkeen tavalliseen kirjekuoreen. Tietoaineiston vastaanottajan on oltava AINA henkilö.

Suojaustason II - III tietoaineistoa voi lähettää vastaanottajalle vahvasti salattuna sähköisen tietojärjestelmän tai verkon välityksellä ja vastaanottaja voi olla henkilö tai organisaatio (ks. ”Sähköpostin ja tiedostojen salaaminen).

Jos sähköisessä muodossa oleva suojaustason II materiaali lähetetään esim. postin välityksellä, käytetään käyttämätöntä tietovälinettä ja tietoaineisto salataan vahvasti (ks. ”Sähköpostin ja tiedostojen salaaminen).

Paperimuotoinen suojaustason II tietoaineisto voidaan lähettää kirjattuna kirjeenä, joka pakataan sinetöityyn mustaan kirjekuoreen tai tietoaineistopussiin ja sen jälkeen tavalliseen kirjekuoreen.

Suojaustason III paperimuotoinen tietoaineisto on suositeltavaa lähettää kirjattuna kirjeenä läpinäkymättömässä kirjekuoressa. Sähköisessä muodossa tallennetut manuaalilähetykset on vahvasti salattava (ks. ”Sähköpostin ja tiedostojen salaaminen).

IV suojaustason tietoaineistoa saa lähettää SM:n hallinnonalan verkossa salaamattomassa muodossa sähköisesti. Jos lähetetään hallinnonalan ulkopuolelle, on lähetys salattava (ks. ”Sähköpostin ja tiedostojen salaaminen).

IV suojaustason tietoaineistoa voidaan lähettää myös faxina, vain jos vastaanottaja on varmistettu. Suojaustason I - III tietoaineistoa ei saa lähettää faxina.

Paperimuotoinen IV suojaustason tietoaineisto voidaan lähettää normaalin postin mukana suljetussa läpinäkymättömässä kirjekuoressa. Sähköisessä muodossa tallennetut manuaalilähetykset on vahvasti salattava (ks. ”Sähköpostin ja tiedostojen salaaminen).
(POHA 2020/2010/4030)

3.3.6 Tietoaineistojen hävittäminen

Hävitettävä sähköisessä tai paperisessa muodossa oleva tietoaineisto hävitetään joko tuhoamalla fyysisesti tai saattamalla sellaiseen muotoon, ettei niiden sisältämää tietoa voida käyttää.

I ja II suojaustason paperiset tietoaineistot hävitetään silppuamalla ne suojaustasovaatimuksen mukaisilla silppureilla ja hävittämisestä tehdään merkintä diaariin. Käytettävästä silppurista pitää löytyä suojaustason I tai II merkintä.

III ja IV suojaustason paperiset tietoaineistot tuhotaan silppuamalla tai keräämällä ne lukittaviin paperinkeräysastioihin.

Tuhottavia asiakirjoja ei tule säilyttää työpisteessä vaan ne tulee työpäivän päätteeksi hävittää silppuamalla taikka toimitettava tarkoitukseen varattuun lukittuun keräysastiaan.

HUOM! Jos et ole varma, kuuluuko hävitettävä paperinen materiaali salassapidon piiriin, on se ensisijaisesti tuhottava silppuamalla taikka laittamalla lukittuun paperinkeräysastiaan (tietoturvalaatikko). ST1 ja ST2 paperinen materiaali on aina tuhottava silppurilla.

Hävitettävät muistivälineet toimitetaan lukittaviin säilytysastioihin ja niiden tuhoaminen tapahtuu keskitetysti. Muistivälineen tietojen poistaminen (deletoiminen) tai muistivälineen alustaminen (formatoiminen) ei tuhoa tiedostoja ja ne ovat edelleen haettavissa esiin.

Käytöstä poistettavat tai huollettavat tietokoneet ja älypuhelimet tai niiden massamuistit toimitetaan yksikössä laitteita koordinoivalle taholle.

(POHA 2020/2010/4030)

Salassa pidettävien tietoaineistojen käsittelystä suojaustasojen mukaan:

Käsittely	**Suojaustaso**			
	IV	III	II	I
Käsittely, laatiminen				
Tietoverkosta erillään oleva poliisihallinnon työasema	Kyllä	Kyllä	Kyllä	Kyllä
Tietoverkkoon kytketty poliisihallinnon työasema	Kyllä	Kyllä	Kyllä	Ei
Poliisihallinnon mobiililaitteet	Kyllä	Kyllä	Ei	Ei
Etäkäyttö	Kyllä	Kyllä	Ei	Ei
Tulostus ja kopiointi				
Verkkotulostin tai verkkoon kytketty monitoimilaite	Kyllä	Kyllä	Ei	Ei
Verkosta erillään oleva tulostin tai monitoimilaite	Kyllä	Kyllä	Kyllä	Kyllä
Kirjaaminen				
Julkinen diaari	Kyllä	Kyllä	Ei	Ei
Salaisten asiakirjojen diaari	Ei	Ei	Kyllä	Ei
Erittäin salaisten asiakirjojen diaari	Ei	Ei	Ei	Kyllä
Lähettäminen				
Kirjaamaton kirje	Kyllä	Ei	Ei	Ei
Kirjattu kirje, huomioitava ST II erityisvaatimukset	Kyllä	Kyllä	Kyllä	Ei
Kuriiriposti, huomioitava ST I ja II erityisvaatimukset	Kyllä	Kyllä	Kyllä	Kyllä
Salaamattomana sähköpostina poliisihallinnon ulkopuolelle	Ei	Ei	Ei	Ei
Salaamattomana sähköpostina poliisihallinnon sisällä	Kyllä	Ei	Ei	Ei
Salattuna sähköpostina	Kyllä	Kyllä	Kyllä	Ei
Fax, vastaanottaja varmistettu	Kyllä	Ei	Ei	Ei
Säilyttäminen, tallentaminen				
Murtosuojattu tila, kuten kassakaappi tai holvi	Kyllä	Kyllä	Kyllä	Kyllä
Lukittu kaappi tai muu vastaava tila	Kyllä	Kyllä	Ei	Ei
Tietoverkkoon kytketty poliisihallinnon työasema	Kyllä	Kyllä	Kyllä	Ei
Tietoverkosta erillään oleva poliisihallinnon työasema	Kyllä	Kyllä	Kyllä	Kyllä
Poliisihallinnon salatut tallennusmediat ja muistilaitteet	Kyllä	Kyllä	Kyllä	Kyllä
Poliisihallinnon mobiililaitteet	Kyllä	Kyllä	Ei	Ei
Hävittäminen				
Paperinkeräys	Ei	Ei	Ei	Ei
Lukittu tietosuojalaatikko ja ulkoisten medioiden lukitut keräyslaatikot	Kyllä	Kyllä	Ei	Ei
Silppuri, huom. silppurin luokitus (taso merkittävä)	Kyllä	Kyllä	Kyllä	Kyllä

Taulukko 7: Poliisin salassa pidettävien tietoaineistojen käsittely (POHA 2020/2010/4030)

4 Toimitilojen turvallisuus osana tietoturvallisuutta

Toimitilojen turvallisuudella varmistetaan, että tietoja, asiakirjoja ja tietokonelaitteita säilytetään ja käsitellään asianmukaisesti turvallisissa tiloissa.

4.1 Kulunvalvonta

Kulunvalvonnalla tarkoitetaan sähköistä järjestelmää, jolla ovien lukitusta ja kulkuoikeuksia hallinnoidaan ja sen avulla varmistetaan, että toimitiloihin ei pääse eikä siellä liiku asiattomia henkilöitä (POHA 2020/2011/3199).

Työhuoneen ovi tulee lukita työpäivän päättyessä tai jos joutuu poistumaan pidemmäksi aikaa työhuoneesta.

Viimeisenä työvuorosta poistuva tarkastaa ikkunoiden sulkemisen ja ovien lukituksen sekä tilat ja poistuu siten, etteivät ovet ja ikkunat jää auki tai lukitsematta ja ettei tiloihin jää asiattomia henkilöitä (POHA 2020/2011/3199).

Kulunvalvonnan piirissä olevia ovia ei saa kiilata auki ja on huolehdittava siitä, että lukittuna tarkoitettuna pidettävät ovet jäävät lukittuun tilaan niistä kulkiessasi.

Liikuttaessa ulko-ovista tai ajoneuvolla autotallin ovista, on pidettävä huoli, ettei ulkopuolisia pääse kulkemaan poliisin tiloihin.

4.2 Ilmoitustaulut ja seinäpinnat

Ilmoitustauluilla ja seinäpinnoilla ei saa säilyttää mitään arkaluontoista tai salaista materiaalia, kuten esimerkiksi kuvia etsintäkuulutetuista henkilöistä. Toimitiloissa liikkuu mm. siivoojia, huoltohenkilökuntaa, vieraita jne. joilla on tiloissa liikkuessaan mahdollisuus nähdä salaista materiaalia.

Jos kokouksessa tms. kirjoitellaan liitu-, fläppi- tai muille tauluille salaista tai luottamuksellista tietoa, tulee ne poistaa ennen kuin huone luovutetaan pois käytöstä.

4.3 Puhtaan pöydän periaate

Työpöydältä tulee kerätä pois luottamukselliset tulosteet sekä muut paperit ja dokumentit viimeistään työpäivän päättyessä siten, että niitä ei jää lojumaan muiden nähtäväksi. Kiinteistössä kulkee mm. siivoojia ja muuta huoltohenkilökuntaa ym. ja vaikka ei olisi syytä epäillä heidän luotettavuuttaan, voivat he nähdä heille kuulumattomia tietoja myös vahingossa. Em. luottamuksellinen ja salassa pidettävä materiaali tulee säilyttää lukitussa laatikossa tai kaapissa.

4.4 Kuulustelutilanteiden tietoturvallisuus

Tietoturvariskien välttämiseksi kuulustelut tulisi suorittaa tätä tarkoitusta varten varatuissa kuulustelutiloissa.

Jos kuitenkin käytetään omaa tai jonkun toisen työhuonetta kuulustelutilana, on pidettävä huoli siitä, että työhuoneen seinillä ja ilmoitustauluilla ei säilytetä mitään arkaluontoista eikä salassa pidettävää materiaalia. Työpöydällä ei saa säilyttää näkyvillä salassa pidettävää materiaalia, jota kuulusteltavan tai avustajan tms. on mahdollista nähdä edes vahingossa.

Jos kuulustelutilanteessa käsitellään salassa pidettävää tietoa, on huolehdittava etteivät sivulliset näe tietoja asiakirjoista tai tietokoneen näytöltä. On myös varottava syöttämästä salasanoja siten, että sivulliset voivat nähdä salasanan esim. sormien liikkeistä.

Kuulusteltavaa tai muitakaan ulkopuolisia henkilöitä ei saa koskaan jättää valvomatta yksin huoneeseen, jos joudutaan poistumaan huoneesta.

4.5 Asiakaspalvelupisteiden tietoturvallisuus

Asiakaspalvelupisteiden seinäpinnoilla ja työpöydillä ei saa säilyttää mitään salassa pidettävää tai muutoin arkaluontoista materiaalia siten, että ne ovat asiakkaiden nähtävillä edes vahingossa. Asiakkaiden asioita hoidettaessa tulee huolehtia siitä, että ulkopuoliset eivät pääse näkemään edes vahingossa muita asiakkaita koskevien dokumenttien sisältöä. Tietokoneen näytöt tulee sijoittaa siten, että asiakkailla eikä muilla ulkopuolisilla ole mahdollisuutta nähdä tietoja tietokoneen näytöltä.

On varmistuttava myös siitä, että asiakkaiden kanssa käytyjä luottamuksellisia keskusteluja eivät ulkopuoliset pääse kuulemaan edes vahingossa.

Työvuoron päättyessä tai muuten poistuttaessa työpisteestä on arkaluontoinen ja salassa pidettävä materiaali laitettava lukittuun laatikkoon tai kaappiin ja tuhottava materiaali on käsiteltävä asianmukaisesti.

4.6 Henkilötunnisteen käyttö

Poliisin tiloissa kulkevat henkilöt on voitava tunnistaa.

Jokaisen poliisissa tai poliisin tiloissa työskentelevän on pidettävä näkyvillä virkamiehen asiointikorttia, virkamerkkiä tai väliaikaista henkilökorttia tai henkilön on muutoin oltava varmuudella tunnistettavissa poliisin henkilökuntaan kuuluvaksi tai tiloissa luvallisesti työskenteleväksi.

Virkapukuisten poliisien osalta nimikyltti on riittävä, ellei toisin määrätä.

(POHA 2020/2011/3199)

4.7 Vierailijakäytäntö

Vierailijan henkilöllisyys on tarkastettava ja hänelle annetaan vierailijatunniste, jos sellainen on poliisilaitoksella käytössä. Vierailijatunniste on pidettävä näkyvillä koko vierailun ajan. Huom. Kaikilla poliisilaitoksilla ei ole käytössä vierailijatunnistetta.

Jokaisella vieraalla tulee olla isäntä, joka vastaa vieraidensa oleskelusta ja kulkemisesta toimitiloissa. Isäntä tai muu henkilökuntaan kuuluva noutaa vieraan ja vierailun päättyessä saattaa tämän pois poliisin tiloista sekä varmistaa vierailijakortin palauttamisen.

Vierasta ei saa koskaan jättää yksin ilman valvontaa työhuoneeseen tai muihin toimitiloihin.

Vierailuihin tulee pyrkiä käyttämään neuvottelutiloja, joissa ei saa olla esillä asiaankuulumatonta materiaalia. Vierailijoiden toimintaa on valvottava myös esim. kännykkäkameroiden käytön suhteen.

Ohjaa vieraat tai eksyneet henkilöt oikeisiin paikkoihin äläkä päästä asiattomia toimitiloihin esimerkiksi töistä lähtiessäsi.
(POHA 2020/2011/3199)

4.8 Kuvaaminen ja valokuvaaminen

Kuvaaminen ja valokuvaaminen poliisin tiloissa on sallittu ainoastaan erillisellä luvalla (POHA 2020/2011/3199). Erityisesti kännykkäkameroiden ja tablettitietokoneiden kameroiden käyttöä on valvottava.

5 Tietokoneen käyttö

Tietojärjestelmiin tarvitaan käyttöoikeus, joka on henkilökohtainen ja se on yhdistetty henkilöllisyyteen ja työtehtäviin (VAHTI 10/2006). Käyttöoikeudet perustuvat todelliseen työtehtävistä johtuvaan tarpeeseen. Tietojärjestelmien käyttöoikeuksista päättävät esimiehet. Käyttöoikeuksia haetaan vain sellaisiin tietojärjestelmiin ja rekistereihin, joita tarvitaan työtehtävissä. Tarpeettomat käyttöoikeudet on pyydettävä poistamaan. Käyttöoikeuksia haetaan Portti -järjestelmän kautta ja esimies vastaa oikeuksien oikeasta laajuudesta. (POHA 2020/2012/946.)

Poistuttaessa tietokoneen ääreltä, on tietokone lukittava tai kirjauduttava ulos järjestelmästä. Työpäivän päättyessä on kirjauduttava ulos ohjelmistoista sekä koneelta. Ole huolellinen tietokoneen käyttäjänä, sillä sinä vastaat omasta koneestasi. (VAHTI 10/2006.)

Tallenna tekemäsi työt koti- tai ryhmälevylle, josta ne varmistetaan keskitetysti. Työasemasi voidaan joutua asentamaan uudestaan esim. vikaantumisen tms. takia, jolloin työaseman omalle C-asemalle tallennetut tiedot menetetään. (Tietoturva - pikaohje 2012.)

Poliisilaitoksen käyttöösi antamaa tietokonetta, työasemaa ja tietovälineitä saa käyttää vain virkatehtävien hoitamiseen, eikä niihin saa itse asentaa mitään ohjelmistoja eikä niiden asetuksiin saa tehdä muutoksia. Älä käytä omia laitteita tai ohjelmistoja virkatehtäviin. (Tietoturva – pikaohje 2012.)

5.1 Asiointikortti

Asiointikortteja ovat virkamerkki, henkilökortti ja muun henkilön kortti. Korttia ja tunnuslukuja on säilytettävä huolellisesti eikä salaisia tunnuslukuja saa luovuttaa toiselle henkilölle. Kortti saa olla kytkettynä tietokoneeseen vain silloin kun kortin haltija on tietokoneen ääressä. Kortti on otettava mukaan koneelta poistuttaessa eikä kortilla saa avata tietokonetta tai yhteyksiä tietokoneella toiselle henkilölle. (POHA 2020/2012/1540.)

Jos virkamerkki, henkilökortti tai muun henkilön kortti katoaa tai se viedään rikoksen kautta, on siitä välittömästi ilmoitettava omaan poliisiyksikköön, jonka jälkeen rekisteröijä ilmoittaa kortin varmenteen sulkulistalle Helpdeskin kautta. Lisäksi asiasta kirjataan aina ilmoitus patjajärjestelmään kadonneen kortin etsintäkuuluttamiseksi. (POHA 2020/2012/1540.)

5.2 Käyttäjätunnus ja salasana

Työasemaan (tietokone) kirjaudutaan asiointikortilla (virkamerkki, henkilökortti tai muun henkilön kortti) ja osa ohjelmista tunnistaa käyttäjän asiointikortin avulla. Osa ohjelmista vaatii vielä erillisen salasanakirjautumisen, jolloin käyttäjät tunnistetaan käyttäjätunnuksen ja salasanan perusteella.

- Käsittele käyttäjätunnusta ja salasanaa samalla tavalla kuin pankkikorttisi tunnuslukua.
- Älä kirjoita salasanaasi muistiin sellaiseen paikkaan, josta se on helposti löydettävissä.
- Älä käytä poliisihallinnon antamaa käyttäjätunnusta ja salasanaa Internetin palveluissa eikä muissakaan käyttäjätunnusta ja salasanaa vaativissa järjestelmissä.
- Kirjaudu koneelle aina ja vain omilla käyttöoikeuksillasi.
- Älä lainaa käyttäjätunnustasi ja salasanaasi kenellekään.
- Älä luovuta salasanojasi edes tietohallinnolle – he eivät niitä tarvitse työssään.
- Kirjautuessasi järjestelmään, pidä huoli siitä, että muut eivät näe salasanaasi.

(VAHTI 10/2006.)

Salasanan tulee olla:

- vähintään kahdeksan (8) merkin mittainen ja
- siinä pitää olla isoja ja pieniä kirjaimia sekä
- numeroita tai erikoismerkkejä
- Siinä ei saa käyttää tuttuja ja jokapäiväisiä sanoja ja sanayhdistelmiä
- ei saa olla missään kielessä esiintyvä sana
- ei saa olla kenenkään nimi (esim. puoliso)
- ei saa olla helposti arvattavissa omasta toiminnasta tai olemuksesta.

Hyvä salasana on sellainen, että sen itse muistaa, mutta ulkopuolisen on vaikea sitä arvata. Jos salasanasta tekee liian vaikean muistaa, niin tällöin on liian suuri kiusaus kirjoittaa se muistiin paperille, jonka joku ulkopuolinen voi saada haltuunsa. (Helsingin yliopisto 2007.)

Hyviä salasanoja voidaan muodostaa esim. seuraavilla tavoilla:

- kaksi toisiinsa liittymätöntä sanaa ja niiden väliin jotain muuta
- jokin sana takaperin kirjoitettuna ja sotkettuna isoilla ja pienillä kirjaimilla ja numeroilla
- jokin sana sotkettuna kirjoitusvirheillä ja numeroilla
- jonkin lauseen sanojen ensimmäisistä kirjaimista muodostettu sekä numero
- satunnaisia kirjaimia ja numeroita, jotka itse muistaa

Huonoja salasanoja ovat mm:

- Antti1 (oma nimi)
- etunimi ja sukunimi yhteen kirjoitettuna
- Roba1 (työpaikka)
- 01011960 (syntymäaika)
- ABC-123 (oman ajoneuvon rekisteritunnus)

Huonon salasanan voi kuka tahansa arvata kohtuullisen helposti ja halutessaan päästä sen avulla käsiksi tiedostoihisi, sähköpostiisi ja tietojärjestelmiin. Helposti arvattava salasana heikentää koko järjestelmän turvallisuutta. (Helsingin yliopisto 2007.)

Vaihda salasanasi, jos epäilet niiden paljastuneen ulkopuolisille. Poliisin keskeiset tietojärjestelmät pakottavat vaihtamaan salasanat määräajoin. Tällöin on hyvä vaihtaa salasanat myös niihin tietojärjestelmiin, jotka eivät pakota salasanaa vaihtamaan.

5.3 Kannettava tietokone

Kannettava tietokone on altis varkauksille ja siksi on syytä pohtia tarvitseeko kannettavaa tietokonetta mukaansa työpaikalta vai ei? Jos kannettavaa tietokonetta ei ole välttämätöntä ottaa mukaan, kannattaa se jättää työpaikalle. Jos se kuitenkin jostain syystä otetaan mukaan työpaikalta, on sen oltava koko ajan henkilökohtaisen valvonnan alla tai sitä on säilytettävä lukitussa ja turvallisessa tilassa. Jos kannettava tietokone on jostain erityisen pakottavasta syystä pakko jättää autoon, sitä ei saa koskaan jättää autoon näkyvälle paikalle, vaan se on laitettava lukittuun tavaratilaan pois näkyviltä.

Kannettavan tietokoneen käytössä työpaikan ulkopuolella on tiedostettava salakatselun mahdollisuus. Salassa pidettäviä tietoaineistoa ei saa tästä syystä käsitellä julkisilla paikoilla tai julkisissa kulkuneuvoissa. Kannettavaa tietokonetta ei saa antaa ulkopuolisten käyttöön, ei edes perheenjäsenille. On myös varmistettava, etteivät esim. perheenjäsenet saa otetuksi yhteyttä poliisin tietojärjestelmiin (VAHTI 3/2002). Jos kannettava tietokone katoaa tai anas-

tetaan, on otettava välittömästi yhteys Helpdeskiin ja oman organisaation tietoturvapäällikköön tai -vastaavaan. Asiasta on kirjattava myös sekalais- tai rikosilmoitus.

Kannettavassa tietokoneessa on käytettävä aina tietokoneen mukana toimitettua näytönsuojakalvoa, kun on salakatselun mahdollisuus. Jos sellaista ei ole koneen mukana toimitettu, voit kysyä sitä Helpdeskistä tai oman organisaatiosi tietoturvapäälliköltä tai -vastaavalta. Huom. kaikkiin kannettaviin tietokoneisiin ei ole saatavilla näytönsuojakalvoa.

5.4 Muistitikku ja muut siirrettävät tietovälineet

Siirrettävällä tietovälineellä tarkoitetaan tietovälinettä, muistivälinettä tai laitetta, johon voidaan tallentaa tietoa ja joka voidaan liittää työasemaan tai palvelimeen tallennetun tiedon lukemista tai kirjoittamista varten (SM 2008/353).

Poliisihallinnon tietoturvaperiaatteet määräyksen (SM 2008/353) mukaan henkilöstö saa käyttää työtehtävissään ainoastaan heidän käyttöönsä luovutettuja, siirrettäviä tietovälineitä. Siirrettävälle tietovälineelle ei saa tallentaa mitään luottamuksellista, ellei tietoja salata vahvasti. Tiedostojen salaamisesta kerrotaan kappaleessa ”Sähköpostin ja tiedostojen salaaminen”. Jos siirrettävä tietoväline on ollut kytkettynä ulkopuoliseen työasemaan tai laitteeseen tai joudutaan jostain syystä käyttämään hallinnon ulkopuolista tietovälinettä, on tietoväline virustarkistettava ennen sen käyttöä poliisilaitoksen työasemissa tai laitteessa. Huom. Salattu muistiväline on ”avattava” ennen virustarkastusta.

Saastumisen leviämisen estämiseksi tarkastusta ei saa suorittaa henkilöiden omilla työasemilla vaan tarkastus tulee mahdollisuuksien mukaan suorittaa poliisiverkosta irrallaan olevalla tietokoneella. Jos on erityinen syy epäillä, että muistivälineessä on tai voi olla haittaohjelma, ei muistivälinettä tulisi kytkeä poliisiverkossa olevaan koneeseen ollenkaan, sillä kaikki haittaohjelmat eivät aiheuta hälytystä. Tällainen muistiväline on toimitettava yksikön tietoturvapäällikölle, paikalliselle tietohallinnolle tai HALTIK:in tukihenkilölle arvioitavaksi ja tarkastettavaksi. Haittaohjelman sisältävän muistivälineen kytkeminen koneeseen saattaa aiheuttaa välittömästi koneen saastumisen ja saastuneet koneet joudutaan asentamaan uudestaan.

Ota selvää, mille työasemalle omassa yksikössäsi on virustarkistuksen tekeminen keskitetty ja käytä tietovälineen tarkistamiseen vain tätä työasemaa.

5.4.1 Muistivälineen tarkistus

Muistivälineen tarkistus suoritetaan Windowsin tiedostonhallinnan kautta valitsemalla kytketty muistiväline ja hiiren oikealla napilla valitsemalla ”Scan ...”. Salattu muistiväline on ”avattava” ennen tarkistusta.

Tarkastetut muistivälineet, joissa on havaittu viruksia, laitetaan käyttökieltoon kunnes muistivälineet on alustettu (formatoitu) uudelleen. Alustus tulee suorittaa täydellisenä eikä ns. pika-alustuksena.

Kun alustus on saatu valmiiksi, tehdään Helpdeskiin palvelupyyntö tarkastukseen käytettävien koneiden uudelleen asentamiseksi.
(Päivitys haittaohjelmatartunnan käsittely 2011)

5.5 Haittaohjelmat

Haittaohjelmat ovat tietokoneohjelmia, jotka tarkoituksellisesti aiheuttavat ei-toivottuja tapahtumia tietokoneessa tai tietojärjestelmässä. Haittaohjelmat voivat kuluttaa kohdekoneen tai tietoverkon resursseja merkittävästi ja ne voivat hidastaa ja jopa estää kokonaan varsinaisen toiminnan. Haittaohjelman saastuttamia järjestelmiä voidaan käyttää laittomiin tarkoituksiin ja ne voivat altistua tietomurroille. Haittaohjelmat voivat lisätä, muuttaa tai tuhota tietojärjestelmässä olevia koneen toiminnalle tärkeitä tai arvokasta informaatiota sisältäviä tietoja. Haittaohjelmat tulevat useimmiten sähköpostin kautta, siirrettävän median mukana taikka Internetin kautta. (VAHTI 3/2004.)

Alla esitellään joitain yleisimpiä haittaohjelmia:

Tietokonevirus on ohjelma, joka monistaa itseään ja leviää tietokoneesta toiseen. Virukset leviävät esim. tietokoneverkon tai tiedontallennusvälineen mukana tulleen tiedoston kautta. (VAHTI 3/2004.)

Mato on samantapainen haittaohjelma kuin virus. Se leviää itsenäisesti ilman aputiedostoa ja se voi levitä nopeasti esim. sähköpostin ja Internetin avulla. Sähköpostimadot voivat olla liitetiedostona tai osana itse viestiä. Ne voivat aktivoitua jo viestin esikatseluvaiheessa tai kun käyttäjä avaa liitetiedoston. (VAHTI 3/2004.)

Troijalainen on ohjelma, joka toimii salassa ohjelman käyttäjältä ja ne leviävät usein jonkun houkuttelevan tai hyödyllisen ohjelman mukana tai ovat osa itse ohjelmaa. Troijalaiset voivat

avata kohdekoneelle takaportin, jonka kautta luvaton tunkeutuja voi päästä murtautumaan tietokoneelle ja etähallitsemaan sitä jopa organisaation palomuurin läpi. Murrettua tietokonetta voidaan käyttää roskapostitukseen, palvelunestohyökkäyksiin tai tietomurtoihin. (VAHTI 3/2004.)

Vakoiluohjelma saattaa sisältyä joihinkin ilmaisiin ja jopa maksullisiin hyöty- ja apuohjelmiin. Vakoiluohjelmat keräävät ja lähettävät tietoa koneesta ja sen käytöstä eteenpäin. Tiedot voivat olla esim. sähköpostisoitteita tai luottokorttitietoja. Vakoiluohjelma voi asentua työasemalle myös salaa käyttäjän tietämättä ja lupaa kysymättä. (VAHTI 3/2004.)

Huijausviesti on tavallisesti sähköpostiviesti, jossa esitetään valheellisia väittämiä esim. viruksista, uudesta treffihuumeesta tms. ja pyydetään vastaanottajaa lähettämään viesti eteenpäin mahdollisimman monelle. Huijausviestit eivät itsessään ole viruksia tai haittaohjelmia, mutta ne kuormittavat turhaan sähköpostiohjelmia. Pahimmillaan huijausviestit erehdyttävät käyttäjää toimimaan virheellisesti, kuten poistamaan käyttöjärjestelmälle tärkeitä tiedostoja viruksina. (VAHTI 3/2004.)

5.5.1 Ohje haittaohjelmien varalle

Poliisin tietoverkossa ja tietojärjestelmissä on toteutettu perustoimenpiteet haittaohjelmien tunnistamiseksi ja poistamiseksi. Pidä itsesi tietoisena noudatettavista menettelyistä ja annetuista ohjeista sekä noudata niitä.

Jos työasemalta löytyy haittaohjelma (virukset, madot, troijalaiset tai muita ei toivottuja ohjelmia), tulee siitä työaseman näytölle asiasta kertova ilmoitus.

Virus ilmoituksen ilmestyessä tietokoneen näytölle, toimi seuraavasti:

1. Paina näytölle ilmestyneen ilmoituksen Close … -painiketta
2. Tallenna ja sulje kaikki avoinna olevat ohjelmat
3. Ilmoita asiasta **heti** HALTIK:n Helpdeskiin
4. Sammuta tietokone
5. Jos joudut lähtemään pois työaseman luota ja se on yhteyskäytössä, jätä koneen päälle lappu jossa kerrotaan että koneesta on löytynyt virus eikä konetta saa käynnistää ennen kuin paikallinen IT-tuki on käynyt paikalla ja ohjeistanut toisin.

TIETOKONETTA EI SAA KÄYTTÄÄ ENNEN IT-TUEN ANTAMAA ERILLISTÄ LUPAA!

Jos koneesta löytyy haittaohjelma, tulee siitä aina ilmoittaa Helpdeskiin ja mielellään myös paikalliselle tietoturvavastaavalle.
(SM 26.4.2006)

6 Internet ja sähköposti

Internetiä ja sähköpostia käytettäessä on hyvä muistaa, että niissä itsessään ei ole minkäänlaista suojausta, vaan tiedot liikkuvat salaamattomina julkisessa verkossa. Internet on työpaikalla tarkoitettu vain työkäyttöön. Muista, että organisaatiosi laitetta, verkkoa tai sähköpostia käyttäessäsi näyt ja esiinnyt tietoverkossa aina organisaation edustajana. Www-sivustojen ylläpitäjät näkevät mistä tulet, joten käytä tutkinnassa ja muutenkin tarvittaessa anonyymeja Internet-työasemia. (VAHTI 10/2006.)

Internetiä käytettäessä on muistettava, että kaikki tiedot tallentuvat selaimen välimuistiin, josta seuraava käyttäjä voi historiatiedoista katsoa, millä sivuilla on käyty aikaisemmin. Selaimen välimuisti on syytä tyhjentää käytön jälkeen, varsinkin jos on esimerkiksi käyty verkkopankissa maksamassa laskuja tms.

Henkilökohtaista virkasähköpostiosoitetta käytetään päivittäiseen virkatehtävien hoitamiseen ja sen käyttöä muuhun tarkoitukseen tulee välttää. Virkasähköpostin välittäminen ja automaattinen ohjaaminen organisaation ulkopuoliseen sähköpostiosoitteeseen on kiellettyä. Varmista, että sähköpostisi käsittelyyn liittyvät velvollisuudet tulevat hoidettua myös poissaolosi aikana virkavelvollisuuksien mukaisesti. Käytä sähköpostin automaattista vastaustoimintoa, jolla lähtee viesti lähettäjälle poissaolosta, sen kestosta ja tieto henkilöstä joka hoitaa sillä aikaa asioita. Laki yksityisyyden suojasta työelämässä, luku 6, käsittelee työnantajan oikeuksia ja mahdollisuuksia työntekijän sähköpostin avaamiseen. (SM 2012/806.)

Mikäli saat toiselle henkilölle kuuluvan sähköpostin, ohjaa viesti oikealle vastaanottajalle ja ilmoita siirrosta sekä vastaanottajan oikea sähköpostiosoite lähettäjälle. Mikäli oikea osoite ei ole tiedossa, on virheellisestä lähetyksestä ilmoitettava viestin lähettäjälle. Muista, että sinulla on vaitiolovelvollisuus ja hyväksikäyttökielto niin viestin sisällöstä kuin sen olemassaolostakin. Varmistu ennen sähköpostin lähettämistä, että sähköposti on kohdistettu oikealle henkilölle ja oikeaan osoitteeseen. (SM 2012/806.)

Muista, että sähköpostin liitetiedostot voivat sisältää haittaohjelmia, joten varo kaikkia epätavallisia sähköposteja ja erityisesti liitetiedostoja. Sähköpostimato voi myös olla osana itse sähköpostiviestiä ja se voi aktivoitua jo viestin esikatseluvaiheessa. Tästä syystä Outlookin (2003) viestin esikatselutoiminto on hyvä poistaa käytöstä seuraavalla tavalla:

1. Klikkaa ylävalikosta Näytä
2. Valitse ja klikkaa Lukuruutu
3. Valitse ja klikkaa Poissa käytöstä

Sähköpostiin tullut roskaposti tulee edelleen lähettää Haltikille toimenpiteitä varten.

Poista roskapostit lukematta (avaamatta) niitä sillä lukeminen kertoo lähettäjälle kyseessä olevan toimiva ja käytössä oleva sähköpostiosoite ja näin sähköpostiisi tuleva roska-postin määrä vain lisääntyy. Lisäksi roskapostit sisältävät usein myös jonkinlaisen haittaohjelman. Roskaposteihin ei pidä myöskään vastata.

Epäilyttävistä viesteistä kuten esim. käyttäjälle kohdennetuista tietojen kalasteluviestistä tulee ilmoitta myös yksikön tietoturvapäällikölle.

6.1 Sähköpostin ja tiedostojen salaaminen

Poliisin salassa pidettävien tietoaineistojen käsittelyohjeen (2020/2010/4030) mukaisesti suojaustasojen II ja III tietoaineistoa sisältävät sähköpostiviestit tulee salata. Suojaustason IV tietoaineistoa sisältävät sähköpostiviestit tulee salata lähetettäessä tietoa hallinnonalan tietoliikenneverkon ulkopuolelle. Hallinnonalan sisäisessä viestinnässä on suositeltavaa käyttää Outlookin salausta, joka tehdään virkakortin varmenteen avulla.

6.1.1 Outlook 2003 ja 2010

Outlookilla voidaan lähettää salattua ja digitaalisesti allekirjoitettua sähköpostia asiointikorttia käyttäen. Salaamalla posti varmistutaan siitä, että viestit liitetiedostoineen ovat vain vastaanottajien käytettävissä. Digitaalisen allekirjoituksen avulla vastaanottaja voi varmistua, että lähettäjä on juuri se keneltä posti on tullut. Salattuja viestejä voi lähettää vastaanottajalle, jolla on virkamiehen asiointikortti tai/ja uudempi sähköinen henkilökortti sekä hakemistoon tallennettu voimassa oleva sähköinen varmennetieto. Outlook on käytännöllisin tapa salata viestit hallinnonalan sisäisessä viestinnässä.

Ohje salatun ja digitaalisesti allekirjoitetun sähköpostin lähettämiseen Outlook 2003:lla löytyy Seitistä.

TUVE -työasemissa (Windows 7) Outlook 2010 -ohje löytyy työpöydällä sijaitsevan ”Työasema-ohjeet” -pikakuvakkeen kautta.

6.1.2 Virkapostilaatikon postin salaus

Outlookissa on mahdollista salata myös virkapostilaatikon (VP) posti sekä ottaa käyttöön digitaalinen allekirjoitus. Virkapostilaatikon salaamiseksi on käyttäjällä oltava kyseisen virkapostilaatikon käsittelyoikeus. (SM:n sähköposti. Virkapostin salaus – käyttäjän ohje 2012.)

Poliisin oma sisäinen varmenne liitetään automaattisesti jokaiseen luotavaan virkapostilaatikkoon. Virkapostilaatikon omistaja tilaa tarvittaessa ulkoisen varmenteen Helpdeskin kautta. Sisäinen varmenne on tarkoitettu hallinnonalan sisällä lähetettävän sähköpostin salaukseen. Ulkoinen varmenne on tarkoitettu hallinnonalan ulkopuolelta tulevan sähköpostin salaukseen ja sitä voidaan käyttää myös hallinnonalan sisäisten sähköpostien salaukseen. (SM:n sähköposti. Virkapostin salaus – käyttäjän ohje 2012.)

Ennen virkapostin salausvarmenteen asentamista on käyttäjän määriteltävä henkilökohtaisen sähköpostin salausasetukset (SM:n sähköposti. Virkapostin salaus – käyttäjän ohje 2012).

Virkapostin salauksen (Outlook 2003) käyttäjän ohje löytyy Seitistä.

TUVE -työasemissa (Windows 7) Outlook 2010 -ohje löytyy työpöydällä sijaitsevan ”Työasemaohjeet” -pikakuvakkeen kautta.

6.1.3 Xxx -järjestelmä

Salassa pidettävien sähköpostiviestien lähettämistä varten on käytössä Xxx -järjestelmä. Se on tarkoitettu erityisesti kansalaisille ja muille ulkopuolisille salassa pidettävän tietoaineiston toimittamista varten. Palvelussa tietoaineiston suojaaminen on toteutettu siten, että sähköposti liitetiedostoineen siirretään ensin palveluntarjoajan turvalliselle palvelimelle, josta vastaanottaja hakee aineiston omatoimisesti salatun yhteyden kautta.

Xxx -järjestelmän käyttö edellyttää käyttöoikeuksien hakemista OIVA:n (Portti) kautta ja hakijalla tulee olla käytössään matkapuhelin, jonka tiedot syötetään OIVA:sssa (Portti)tarkoitusta varten varattuun kenttään. Myös viestin vastaanottajalla tulee olla käytössään matkapuhelin. Xxx -järjestelmän käyttöohjeet löytyvät Seitistä.

6.1.4 Yyy -salausohjelmisto

Ohjelmistolla voidaan salata yksittäisiä tiedostoja ja toimittaa esimerkiksi sähköpostin liitteenä. Ohjelman voi tehtävissään tarvitseva tilata omalle työasemalleen Helpdeskin kautta Haltikista. Yyy -salausohjelmiston käyttöohjeet löytyvät Seitistä.

7 Matkapuhelin

Matkapuhelin on tarkoitettu vain virkakäyttöön ja sitä on säilytettävä huolellisesti, ettei se joudu ulkopuolisten haltuun. Pin-koodin oletusasetus tulee vaihtaa puhelimen käyttöönottohetkellä ja pin-koodin kysely tulee pitää käytössä. Perusmatkapuhelimessa on suositeltavaa käyttää puhelimen automaattista lukitusta (suojakoodi), joka lukitsee puhelimen, kun se on ollut käyttämättömänä ennalta määritellyn ajan, esim. 5 minuuttia. (Poliisihallitus 2020/2011/337.)

Mobiilipostin ja kalenterin käyttämiseen tarvittava puhelin on erikseen määritelty vakioitu älypuhelin, joka sisältää riittävät turvallisuusominaisuudet kuten muistin salaus, etähallittavuus ja suojakoodin pakollinen käyttö. Sähköpostin ja kalenteritoimintojen käyttämisessä älypuhelimella on noudatettava samaa huolellisuutta kuin käytettäessä tietokoneella olevaa sähköposti- ja kalenteriohjelmaa. (Poliisihallitus 2020/2011/337.)

Jos mobiilipostilla varustettu puhelin katoaa tai anastetaan, voidaan puhelin ja sen palvelut sulkea operaattorin toimesta etäkomennolla. Sulkemispyyntö operaattorille tehdään Haltikin Helpdeskin kautta. Jos SIM-kortti on operaattorin toimesta ehditty lukita, ei etävalvonta eikä etähallinta toimi. Tavallisen peruspuhelimen kadotessa liittymä suljetaan operaattorille tehtävällä pyynnöllä, jonka tekemisestä vastaa puhelimen käyttäjä. (Poliisihallitus 2020/2011/337.)

Matkapuhelimen katoamisesta on ilmoitettava myös yksikön puhelinyhdyshenkilölle ja anastustapauksessa on asiasta tehtävä rikosilmoitus. Jos matkapuhelimeen tulee vikaa, toimitetaan se huoltoon yksikön puhelinyhdyshenkilön toimesta. Matkapuhelimen vikaantumiseen tai katoamiseen on hyvä varautua varmuuskopioimalla matkapuhelimen tiedot työasemalla tai erilliselle muistivälineelle. (Poliisihallitus 2020/2011/337.)

Jos matkapuhelin kytketään työasemaan esim. valokuvien siirtoa varten, tulee puhelin (muisti ja muistikortti) tarkastaa haittaohjelmien varalta. Tarkastus suoritetaan kytkemällä matkapuhelin tietokoneen USB-porttiin ja suorittamalla virustarkastus samoin kuin edellä siirrettävälle tietovälineelle. (Poliisihallitus 2020/2011/337.)

Haittaohjelmien leviämisen estämiseksi vastaa kaikkiin puhelimen näyttöön tuleviin ohjelmien asennusta ja asetusten muutoksia ehdottaviin ilmoituksiin EI. Jos epäilet, että matkapuhelimeesi on asentunut jokin haittaohjelma, kytke puhelimesta virta pois ja toimita puhelin yksikön IT-tukeen tarkastettavaksi. (Poliisihallitus 2020/2011/337.) Bluetooth on yleisin haittaohjelmien leviämiskanava, joten puhelimen bluetooth –tila on syytä pitää piilotettuna muille bluetoothlaitteille (VAHTI 2/2007).

Puhuttaessa työasioita matkapuhelimessa on varmistuttava, etteivät ulkopuoliset pääse kuulemaan luottamuksellisia keskusteluja. Salassa pidettäviä tietoja ei saa puhua julkisilla paikoilla ettei kukaan ulkopuolinen pääse niitä kuulemaan edes vahingossa.

8 VIRVE –radio

Poliisin VIRVE-toimintaohje (2020/2011/1496) ja sen liitteenä oleva ohje: ”Poliisin VIRVE-toimintaohje” sisältävät ohjeet poliisin VIRVE-käytöstä. Ohje sisältää myös tietoturvallisuuteen liittyvän ohjeistuksen.

Ohjetta jaettaessa ja käsiteltäessä on otettava huomioon, että se sisältää luottamukselliseksi turvaluokiteltua (ST III) tietoa, joka ei saa joutua poliisin ulkopuolisten tahojen haltuun. Tästä syystä ohjeen sisältöä ei voida tässä tietoturvaohjeessa käsitellä. Ohje on löydettävissä poliisin sisäisestä Intra -verkosta (Seitti).

9 Ajoneuvossa työskentely

- Kirjautuessasi tietokoneelle, huolehdi siitä, että ulkopuoliset eivät pääse näkemään käyttäjätunnustasi ja salasanaasi.
- Huolehdi siitä, että ulkopuoliset eivät pääse näkemään tietoja tietokoneen näytöltä.
- Jos ajoneuvon välitilassa on erillinen tietokoneen näyttö, huolehdi siitä, että sen näytöltä eivät ulkopuoliset pääse näkemään tietoja.
- Ajoneuvoradio (VIRVE) ei saa olla niin lujalla, että ulkopuolisilla on mahdollisuus kuulla radioliikennettä.
- Älä säilytä arkaluontoisia muistiinpanoja ajoneuvon kojelaudalla tai muualla siten, että ulkopuolisilla on mahdollisuus niitä nähdä.
- Lukitse ajoneuvon työasema ja ovet aina kun poistut ajoneuvosta ja sen lähettyviltä niin että ajoneuvo ei ole kontrollissasi.
- Työvuoron päätteeksi kirjaudu ulos tietokoneelta ja kerää ajoneuvosta pois kaikki sinne kuulumaton arkaluontoinen materiaali ja toimita se asianmukaisiin paikkoihin - säästettävät lukittuun laatikkoon kaappiin tms. ja hävitettävä materiaali silppuriin tai lukittuihin silppurilaatikoihin.

10 Yleisellä paikalla työskentely

- Yleisellä paikalla on huolehdittava siitä, että ulkopuoliset eivät pääse kuulemaan poliisin radioliikennettä.
- Käytä VIRVE-radiossa korvakuuloketta aina kun se on mahdollista.
- Arkaluontoisia tietoja käsiteltäessä on huolehdittava, että ulkopuoliset eivät pääse niitä näkemään tai kuulemaan.
- On myös huomioitava ST I - IV luokiteltujen asiakirjojen ja tietojen käsittelyvaatimukset.

11 Sosiaalinen media ja -hakkerointi

Poliisihallinnon edustajat sosiaalisessa mediassa ovat erikseen nimettyjä ja koulutettuja henkilöitä, muut toimivat yksityiskäyttäjinä eivätkä edusta työnantajaansa.

Ohjeita sosiaalisen median käytön tueksi:

1. Selvitä ja noudata poliisihallinnon tietoturvaperiaatteita ja muuta ohjeistusta sekä määräystä poliisin näkyvästä toiminnasta sosiaalisessa mediassa.
2. Jos mainitset sosiaalisessa mediassa esim. henkilöprofiilissasi tai muutoin työnantajaksi poliisihallinnon, esiinnyt tällöin kansalaisen silmissä poliisin epävirallisena edustajana vaikka toimisitkin omasta ja työnantajan kannalta yksityiskäyttäjänä. Muista käyttäytyä sen mukaisesti.
3. Osalle henkilöstöstä jo pelkkä maininta kuulumisesta poliisihallintoon saattaa aiheuttaa turvallisuusriskin henkilön tai hänen läheistensä turvallisuudelle. Kunnioita työkavereidesi työtehtäviä ja tahtoa äläkä kutsu tai nimeä heitä palveluihin tai ryhmiin ilman lupaa.
4. Mieti tarkkaan, mitä tietoja itsestäsi syötät sosiaalisen median palveluihin. - Kerran nettiin laitettu tieto pysyy siellä ikuisesti ja saattaa siis vaikuttaa tulevaisuudessa elämääsi.
5. Tarkista käyttäjäprofiilin yksityisyyden suojaa koskevat asetukset ja muuta niitä tarvittaessa siten, että tietosi eivät leviä laajemmalle kuin haluamallesi käyttäjäjoukolle - Et voi koskaan täysin kontrolloida kenelle tietosi lopulta päätyvät.
6. Älä käytä samoja käyttäjätunnuksia ja salasanoja poliisin tietojärjestelmissä kuin sosiaalisen median tai muissa vapaa-ajan palveluissa. Huolehdi salasanasi laadusta käyttämällä vain vahvoja salasanoja.

7. Älä klikkaile hämäräperäisiä linkkejä palveluissa. Sosiaalisessa mediassa haittaohjelmat leviävät helposti mm. siksi että ne näyttävät tulevan tutulta henkilöltä jolloin niihin luotetaan paremmin.
8. Älä keskustele työasioista sosiaalisissa medioissa. Ole erityisen huolellinen salassa pidettävän tiedon suhteen. Muista, että palvelun ylläpitäjät pääsevät teknisesti käsiksi kaikkeen palveluun talletettuun ja myös vain keskustelun osapuolten väliseksi tarkoitettuun tietoon. Viestien ja tietojen säilymiseen kahdenkeskisenä ei ole mitään takeita.
9. Jos epäilet, että olet joutunut huijatuksi tai muun hyökkäyksen kohteeksi, älä epäröi pyytää apua. Älä jätä tekemättä asiasta rikosilmoitusta, vaikka taloudellinen menetys saattaa osaltasi jäädä vaatimattomaksi.

(Mukailtu poliisihallinnon henkilöstön sosiaalisen median 15 tietoturvaperiaatetta 2011 – ohjeesta)

Sosiaalisessa hakkeroinnissa käytetään hyväksi vakuuttavaa esiintymistaitoa, ympäri puhumista ja muita sosiaalisia taitoja henkilön manipuloimiseksi luovuttamaan arkaluontoisia tietoja ulkopuolisille. Mikä tahansa puhelinsoitto, sähköposti- tai muu yhteydenotto voi olla sosiaalinen hakkerointiyritys. Kaikkiin yhteydenottoihin ja tietojen kyselyihin tulee suhtautua varauksella ja tervettä järkeä käyttäen ja aina ennen tiedon luovuttamista tulee tarkoin miettiä, onko kyseessä arkaluontoinen tai salassa pidettävä tieto ja onko tiedon vastaanottajalla oikeus tähän tietoon. (Tietoviikko 2011.)

Sosiaalinen media on vienyt sosiaalisen hakkeroinnin käyttömahdollisuudet uudelle tasolle, sillä yhteisöpalvelut (esim. Facebook, Twitter ym.) lisäävät ihmisten luottamuksen tunnetta toisiin. Ihmiset ovat yhä innokkaampia ja avoimempia jakamaan henkilökohtaisia ja muitakin tietojaan verkossa erilaisten yhteisöpalvelujen kautta. Sosiaalisessa mediassa ei saa puhua työasioista eikä siellä kannata jakaa henkilökohtaisia tietojaan edes ystävien nähtäväksi, sillä kaikki mitä verkkoon ja yhteisöpalveluihin kirjoitetaan, jää sinne pysyvästi ja on sieltä ulkopuolisten löydettävissä. (Tietoviikko 2011.)

12 Toiminta ongelmatilanteissa ja ilmoitusvelvollisuus

Tietoturvallisuus perustuu lainsäädäntöön ja normiohjaukseen. Vastuu tietoturvallisuudesta ja siihen liittyvä osaaminen kuuluu omalta osaltaan jokaiselle. Ilmoita aina tietoturvallisuuteen liittyvistä ongelmatilanteista ja havaitsemistasi uhkista ja suojauspuutteista välittömästi tietoturvapäällikölle tai -vastaavalle tai omalle esimiehellesi. Heidän velvollisuutensa on ryhtyä

tarvittaviin toimenpiteisiin. Pyydä tarvittaessa neuvoa tietoturvapäälliköltä tai turvallisuus-päälliköltä.

Kiireellisten tietoturvaan liittyvien ilmoitusten lisäksi on asiasta tehtävä poikkeamatilanneil-moitus, joka löytyy Seitin Tietopankista.

13 Tietoturvallisuuden huoneentaulu

Tietoturvallisuuden huoneentaulu

- Tutustu poliisin yleisiin sekä poliisilaitoksen/-yksikkösi tietoturvaohjeisiin ja osallistu tarjottuun koulutukseen.
- Poliisin tiloissa kulkiessasi pidä virkamerkkisi tai kuvallinen henkilökorttisi näkyvillä.
- Älä jätä vieraitasi yksin työhuoneeseesi tai muihin poliisilaitoksen tiloihin.
- Älä anna ulkopuolisten käyttää tietokonettasi.
- Noudata ns. puhtaan pöydän periaatetta eli älä säilytä työpöydälläsi salassa pidettävää aineistoa.
- Lukitse työhuoneesi ovi poistuessasi huoneesta.
- Älä luovuta henkilökohtaisia käyttäjätunnuksia ja salasanojasi toisen henkilön käyttöön – Ei edes tietohallintohenkilöstölle, koska he eivät niitä tarvitse.
- Älä anna ulkopuolisten nähdä tietokoneesi näyttöä tai näppäimistöä, kun käsittelet arkaluonteista tietoa tai kun syötät käyttäjätunnuksia ja salasanoja.
- Vaihda salasanasi kun epäilet niiden paljastuneen.
- Käytä tietoaineistoa ja työvälineitä vain työtehtäviesi hoitamiseen.
- Tallenna tekemäsi työ verkkoaseman levylle, mistä tiedot varmistetaan keskitetysti.
- Varmista aina, mihin verkkotulostimeen tulostat ja hae tulosteesi verkkotulostimesta heti tulostuksen jälkeen.
- Mikäli siirrät aineistoa muistitikun tai muun muistivälineen avulla, valvo siirtoa aina henkilökohtaisesti.
- Estä asiaton pääsy tietojärjestelmiin kirjautumalla ulos työasemalta tai lukitsemalla työasemasi aina kun poistut työpisteestäsi.
- Käsittele tietoja huolellisesti välineestä riippumatta – olipa tiedon välittäjänä sitten henkilö, tietokone, paperi, puhelin tai faxi.
- Ilmoita aina tietoturvallisuuteen liittyvistä ongelmatilanteista ja havaitsemistasi uhkista ja suojauspuutteista välittömästi tietoturvapäällikölle/ -vastaavalle tai omalle esimiehellesi.
- Pyydä tarvittaessa neuvoa tietoturvapäälliköltä, turvallisuuspäälliköltä tai IT-tuelta.

Oman yksikön tietoturvavastaavat

Nimi	**Yksikkö**	**puh.**	**Huom.**

Lähteet

Haittaohjelmilta suojautumisen yleisohje. 2004. Vahti 3/2004. Helsinki: Valtiovarainministeriö.

Henkilöstön tietoturvaohje. 2006. Vahti 10/2006. Helsinki: Valtiovarainministeriö.

Henkilötietolaki 523/1999. Viitattu 20.10.2011.
http://www.finlex.fi/fi/laki/alkup/1999/19990523

Hyvä salasana. Helsingin yliopisto 2007. Viitattu 1.10.2012.
http://www.helsinki.fi/helpdesk/ohjeet/kayttoluvat_ja_salasanat/salasanat/hyva_salasana.html

Laki henkilötietojen käsittelystä poliisitoimessa 761/2003. Viitattu 20.10.2011.
http://www.finlex.fi/fi/laki/alkup/2003/20030761

Laki viranomaisen toiminnan julkisuudesta 621/1999. Viitattu 20.10.2011.
http://www.finlex.fi/fi/laki/alkup/1999/19990621

Mitä tehdä jos työasemalta löytyy haittaohjelma. 26.4.2006. Liite: Käyttäjän ohje. 2011. Helsinki: Sisäasiainministeriö. Poliisiosasto.

Määräys poliisin salassa pidettävien tietoaineistojen käsittelystä 2020/2010/4030 (1.1.2011 – toistaiseksi). Helsinki: Poliisihallitus.

Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. 2010. Vahti 2/2010. Helsinki: Valtiovarainministeriö.

Outlook 2003 - Salatun ja digitaalisesti allekirjoitetun sähköpostin lähettäminen. Ohje (versio 1.4). 2009. Rovaniemi: Hallinnon tietotekniikkakeskus.

Poliisihallinnon henkilöstön sosiaalisen median 15 tietoturvaperiaatetta. Helsinki: Poliisihallitus.

Poliisihallinnon tietoturvaperiaatteet määräys SMDno/2008/353 (7.8.2008 – 6.8.2013). Helsinki: Sisäasiainministeriö. Poliisiosasto.

Poliisin henkilökortti- ja virkamerkkimääräys 2020/2012/1540 (11.4.2012 - 31.12.2015). Helsinki: Poliisihallitus.

Poliisin puhelinohje 2020/2011/337 (30.5.2011 - 30.4.2016). Helsinki: Poliisihallitus.

Poliisin tietoturvapolitiikka määräys 2020/2010/4157 (1.1.2011 – 1.1.2016). Helsinki: Poliisihallitus.

Poliisin VIRVE-toimintaohje. 2020/2011/1496. Helsinki: Poliisihallitus.

Päivitys haittaohjelmatartunnan käsittely 17.11.2011. Ohje. Helsingin poliisilaitos.

Sisäasiainministeriön hallinnonalan sähköpostin käyttöpolitiikka. Määräys. SMDno/2012/806. Luonnos.

Sisäasiainministeriön sähköposti. Virkapostin salaus - käyttäjän ohje. versio 1.1 (26.3.2012). Haltik.

Tietoturva -pikaohje/HPL. Helsingin poliisilaitos. 2012.

Tietoturvallisuus. Julkisen hallinnon ICT. Valtiovarainministeriö. Viitattu 11.3.2012. http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/02_tietoturvaohjeet_ja_maaraykset/index.jsp

Tietoturvatasot poliisihallinnossa määräys 2020/2011/81 (11.1.2011 – 31.12.2015). Helsinki: Poliisihallitus.

Tietoviikko. 2011. Yrityksen viisi suurinta sosiaalisen median tietoturvauhkaa. Artikkeli. 31.5.2011. Toimittaja: Rinta, N. Talentum. Viitattu 22.10.2012. http://www.tietoviikko.fi/kaikki_uutiset/yrityksen+viisi+suurinta+sosiaalisen+median+tietoturvauhkaa/a635238

Turvallisuuskäytännöt poliisin tiloissa ohje 2020/2011/3199 (x.x.2012 - toistaiseksi). Helsinki: Poliisihallitus.

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681. Viitattu 20.10.2011. http://www.finlex.fi/fi/laki/ajantasa/2010/20100681

Valtionhallinnon etätyön tietoturvallisuusohje. 2002. Vahti 3/2002. Helsinki: Valtiovarainministeriö.

Älypuhelimien tietoturvallisuus – hyvät käytännöt. 2007. Vahti 2/2007. Helsinki: Valtiovarainministeriö.

Taulukot

Kuvat